NEC

US300c
ユーザーズガイド

856-129025-018-00
2010年　7月　初版

商標について

MicrosoftおよびWindowsは、Microsoft Corporationの登録商標です。

オペレーティングシステムの表記について

Windows Server 2003はMicrosoft® Windows® Server 2003, Standard Edition operating systemおよびMicrosoft® Windows® Server 2003, Enterprise Edition operating systemの略です。Windows 2000はMicrosoft® Windows® 2000 Server operating systemおよびMicrosoft® Windows® 2000 Advanced Server operating system、Microsoft® Windows® 2000 Professional operating systemの略称です。Windows XPはMicrosoft® Windows® XP Home Edition operating systemおよびMicrosoft Windows XP Professional operating systemの略です。Windows XP EmbeddedはMicrosoft® Windows® XP Embeddedの略称です。Windows NTはMicrosoft® Windows NT® Server network operating system version 3.51/4.0およびMicrosoft® Windows NT® Workstation operating system version 3.51/4.0の略称です。Windows MeはMicrosoft® Windows® Millennium Edition operating systemの略称です。Windows 98はMicrosoft® Windows®98 operating systemの略称です。Windows 95はMicrosoft® Windows®95 operating systemの略称です。Windows CE 5.0はMicrosoft® Windows® CE Version5.0の略称です。
Windows Embedded StandardはMicrosoft® Windows® Embedded Standard の略称です。

ご注意

(1)　本書の内容の一部または全部を無断転載することは禁止されています。
(2)　本書の内容に関しては将来予告なしに変更することがあります。
(3)　弊社の許可なく複製・改変などを行うことはできません。
(4)　本書は内容について万全を期して作成いたしましたが、万一ご不審な点や誤り、記載もれなどお気づきのことがありましたら、お買い求めの販売店にご連絡ください。
(5)　運用した結果の影響については(4)項にかかわらず責任を負いかねますのでご了承ください。

このユーザーズガイドは、必要なときすぐに参照できるよう、お手元に置いておくようにしてください。「使用上のご注意」を必ずお読みください。

⚠ 使用上のご注意 - 必ずお読みください -

本製品を安全に正しくご使用になるために必要な情報が記載されています。また、本文中の名称については2ページの「各部の名称と機能」をご参照ください。

安全にかかわる表示について

本製品を安全にお使いいただくために、このユーザーズガイドの指示に従って操作してください。

このユーザーズガイドには本製品のどこが危険か、どのような危険に遭うか、どうすれば危険を避けられるかなどについて説明されています。

ユーザーズガイドでは、危険の程度を表す言葉として、「警告」と「注意」という用語を使用しています。それぞれの用語は次のような意味を持つものとして定義されています。

人が死亡する、または重傷を負うおそれがあることを示します。

⚠ 注意

火傷やけがなどを負うおそれや物的損害を負うおそれがあることを示します。

危険に対する注意・表示は次の3種類の記号を使って表しています。それぞれの記号は次のような意味を持つものとして定義されています。

記号		説明	例
△	**注意の喚起**	この記号は危険が発生するおそれがあることを表します。記号の中の絵表示は危険の内容を図案化したものです。	(例) (感電注意)
⃠	**行為の禁止**	この記号は行為の禁止を表します。記号の中や近くの絵表示は、してはならない行為の内容を図案化したものです。	(例) (分解禁止)
●	**行為の強制**	この記号は行為の強制を表します。記号の中の絵表示は、しなければならない行為の内容を図案化したものです。危険を避けるためにはこの行為が必要です。	(例) (プラグを抜け)

(ユーザーズガイドでの表示例)

本書と警告ラベルで使用する記号とその内容

注意の喚起

記号	内容	記号	内容
	感電のおそれのあることを示します。		発煙または発火のおそれがあることを示します。
	爆発または破裂のおそれがあることを示します。		けがをするおそれがあることを示します。
	特定しない一般的な注意・警告を示します。		

行為の禁止

記号	内容	記号	内容
	本製品を分解・修理・改造しないでください。感電や火災のおそれがあります。		水や液体がかかる場所で使用しないでください。水にぬらすと感電や発火のおそれがあります。
	指定された場所には触らないでください。感電や火傷などの傷害のおそれがあります。		火気に近づけないでください。発火するおそれがあります。
	ぬれた手で触らないでください。感電するおそれがあります。		特定しない一般的な禁止を示します。

行為の強制

記号	内容	記号	内容
	本製品の電源プラグをコンセントから抜いてください。火災や感電のおそれがあります。		特定しない一般的な使用者の行為を指示します。説明に従った操作をしてください。
	必ず接地してください。感電や火災のおそれがあります。		

安全上のご注意

本製品を安全にお使いいただくために、ここで説明する注意事項をよく読んでご理解し、安全にご活用ください。記号の説明についてはiiiページの『安全にかかわる表示について』の説明を参照してください。

全般的な注意事項

警告

人命に関わる業務や高度な信頼性を必要とする業務には使用しない

本製品は、医療機器・原子力設備や機器、航空宇宙機器・輸送設備や機器など、人命に関わる設備や機器および高度な信頼性を必要とする設備や機器などへの組み込みやこれらの機器の制御などを目的とした使用は意図されておりません。これら設備や機器、制御システムなどに本製品を使用した結果、人身事故、財産損害などが生じても弊社はいかなる責任も負いかねます。

煙や異臭、異音がしたまま使用しない

万一、煙、異臭、異音などが生じた場合は、ただちに電源をOFFにして電源プラグをコンセントから抜いてください。その後、お買い求めの販売店または保守サービス会社にご連絡ください。そのまま使用すると火災の原因となります。

針金や金属片を差し込まない

通気孔やUSBコネクタ等のすきまから金属片や針金などの異物を差し込まないでください。感電の危険があります。

注意

海外で使用しない

本製品は、日本国内専用の装置です。海外では使用できません。この装置を海外で使用すると火災や感電の原因となります。

本製品内に水や異物を入れない

本製品内に水などの液体、ピンやクリップなどの異物を入れないでください。火災や感電、故障の原因となります。もし入ってしまったときは、すぐ電源をOFFにして、電源プラグをコンセントから抜いてください。分解しないで販売店または保守サービス会社にご連絡ください。

電源・電源コードに関する注意事項

⚠警告

ぬれた手で電源プラグを持たない

ぬれた手で電源プラグの抜き差しをしないでください。感電するおそれがあります。

アース線をガス管につながない

アース線は絶対にガス管につながないでください。ガス爆発の原因になります。

⚠注意

指定以外のコンセントに差し込まない

指定された電圧でアース付のコンセントをお使いください。指定以外で使うと火災や漏電の原因となります。また、延長コードが必要となるような場所には設置しないでください。本製品の電源仕様に合っていないコードに接続すると、コードが過熱して火災の原因となります。

たこ足配線にしない

コンセントに定格以上の電流が流れることによって、過熱して火災の原因となるおそれがあります。

中途半端に差し込まない

電源プラグは根元までしっかりと差し込んでください。中途半端に差し込むと接触不良のため発熱し、火災の原因となることがあります。また差し込み部にほこりがたまり、水滴などが付くと発熱し、火災の原因となるおそれがあります。

指定以外の電源コードを使わない

本製品に添付されている電源コード以外のコードを使わないでください。電源コードに定格以上の電流が流れると、火災の原因となるおそれがあります。また、電源コードの破損による感電や火災を防止するために次の注意をお守りください。

- コード部分を引っ張らない。
- 電源コードを折り曲げない。
- 電源コードをねじらない。
- 電源コードを踏まない。
- 電源コードを束ねたまま使わない。
- 電源コードをステープラ等で固定しない。
- 電源コードをはさまない。
- 電源コードに薬品類をかけない。
- 電源コードの上にものを載せない。
- 電源コードを改造・加工・修復しない。
- 損傷した電源コードを使わない。（損傷した電源コードはすぐ同じ規格の電源コードと取り替えてください。交換に関しては、お買い求めの販売店または保守サービス会社にご連絡ください。）

添付の電源コードを他の装置や用途に使用しない

添付の電源コードは本製品に接続し、使用することを目的として設計され、その安全性が確認されているものです。決して他の装置や用途に使用しないでください。火災や感電の原因となるおそれがあります。

ケーブル部分を持って引き抜かない

ケーブルを抜くときはコネクタ部分を持ってまっすぐに引き抜いてください。ケーブル部分を持って引っ張ったりコネクタ部分に無理な力を加えたりするとケーブル部分が破損し、火災や感電の原因となります。

設置・移動・保管・接続に関する注意事項

⚠ 注意

指定以外の場所に設置・保管しない

本製品を次に示すような場所や本書で指定している場所以外に置かないでください。火災の原因となるおそれがあります。

- ほこりの多い場所。
- 給湯器のそばなど湿気の多い場所。
- 直射日光が当たる場所。
- 不安定な場所。

腐食性ガスの存在する環境で使用しない

腐食性ガス(塩化ナトリウムや二酸化硫黄、硫化水素、二酸化窒素、塩素、アンモニア、オゾンなど)の発生する場所に設置し、使用しないでください。また、ほこり中に腐食を促進する成分(硫黄など)や導電性の金属などが含まれている環境へも設置しないでください。装置内部のプリント板が腐食・ショートし、火災の原因となるおそれがあります。ご不明の点はお買い求めの販売店、または保守サービス会社にお問い合わせください。

電池に関する注意事項

⚠警告

電池は火の中に入れない

火の中に入れたり、加熱したりすると爆発したり、破裂したりするおそれがあります。

電池を分解、改造しない

分解、改造すると破裂したり、液もれするおそれがあります。弊社指定以外の電池は、品質、性能、安全性について保証の対象外となります。

⚠注意

電池はお子さま、特に乳幼児の手の届かない場所に保管する

電池内部には、有害物質を含んでいるため、誤って飲み込んだり、なめたりすると危険です。万一、飲み込んだ場合は、直ちに医師にご相談ください。

運用中の注意事項

⚠注意

雷が鳴ったら触らない

雷が発生しそうなときは電源プラグをコンセントから抜いてください。また電源プラグを抜く前に、雷が鳴りだしたら、ケーブル類も含めて本製品には触れないでください。火災や感電の原因となります。

ペットを近づけない

本製品にペットなどの生き物を近づけないでください。排泄物や体毛が本製品内部に入って火災や感電の原因となります。

通気開口部をふさがない

内部に熱がこもり、発煙、発火の原因となるおそれがあります。

ヘッドフォンを耳に当てたまま接続しない

ヘッドフォンを耳に当てたままヘッドフォン端子に接続しないでください。耳を痛めるおそれがあります。また、接続前にボリュームが大きくなっていないことを確認してください。

通気開口部に注意する

通気開口部とその周辺は、室温よりも高い温度となっております。長時間触れていると、低温やけどのおそれがありますので、肌の弱い方などは特にご注意ください。

無線機能使用に関する注意事項

⚠警告

埋め込み型心臓ペースメーカー装着部から30cm以上離して使用する

埋め込み型心臓ペースメーカーを装着されている方は、本製品を心臓ペースメーカー装着部から30cm以上離して使用してください。電波により影響を受けるおそれがあります。

医療機関など本製品の使用を禁止した区域では本製品の電源または無線機能をOFFにする

医療機関などで本製品の使用を禁止した区域では、本製品の電源をOFFにするか、無線LANなどの無線機能をOFFにしてください。また、医療機関などで本製品の使用を認めた区域でも、近くで医療機器が使用されている場合には、本製品の電源をOFFにするか、無線LANなどの無線機能をOFFにしてください。医療機器に影響を与え、事故の原因になることがあります。詳しい内容については、各医療機関にお問い合わせください。

他の機器に電波障害を引き起こした場合は本製品の無線機能をOFFにする

本製品の無線機能を使用中に、他の機器に電波障害を引き起こした場合は、速やかに無線機能をOFFにするか、本製品の使用を中止してください。機器に影響を与え、誤動作による事故の原因になるおそれがあります。

お手入れに関する注意事項

⚠警告

自分で分解・修理・改造はしない

絶対に分解したり、修理・改造を行ったりしないでください。本製品が正常に動作しなくなるばかりでなく、感電や火災の危険があります。

プラグを差し込んだまま取り扱わない

お手入れや装置に接続されているケーブルの取り付け/取り外しは、本製品の電源をOFFにして、電源プラグをコンセントから抜いて行ってください。たとえ電源をOFFにしても、電源コードを接続したまま本製品内の部品に触ると感電するおそれがあります。
また、電源プラグはときどき抜いて、乾いた布でほこりやゴミをよくふき取ってください。ほこりがたまったままで、水滴などが付くと発熱し、火災の原因となるおそれがあります。

取り扱い上のご注意

本製品を正しく動作させるために次に示す注意事項をお守りください。これらの注意を無視した取り扱いをすると本製品の誤動作や故障の原因となります。

- 本製品の電源を一度OFFにした後、再びONにするときは10秒以上経過してからにしてください。無停電電源装置(UPS)に接続している場合も10秒以上経過してからONになるようにスケジューリングの設定をしてください。
- 本製品を移動する前に電源をOFFにして、電源プラグをコンセントから抜いてください。
- 定期的に本製品を清掃してください。定期的な清掃はさまざまな故障を未然に防ぐ効果があります。
- 落雷等が原因で瞬間的に電圧が低下することがあります。この対策として無停電電源装置等を使用することをお勧めします。
- 本製品を正しく動作させるためにも室温を保てる場所に保管することをお勧めします。装置を保管する場合は、保管環境条件(温度：-20℃～60℃、湿度：20%～80%)を守って保管してください(ただし、結露しないこと)。
- 本製品のそばでは携帯電話やPHS、ポケットベルの電源をOFFにしておいてください。電波による誤動作の原因となります。
- インタフェースケーブルの取り扱いや接続について次の注意をお守りください。
  - 破損したケーブルコネクタを使用しない。
  - ケーブルを踏まない。
  - ケーブルの上にものを載せない。
  - ケーブルの接続がゆるんだまま使用しない。
  - 破損したケーブルを使用しない。
- 本装置、内蔵型のオプション機器などは、寒い場所から暖かい場所に急に持ち込むと結露が発生し、そのまま使用すると誤作動や故障の原因となります。保管した大切なデータや資産を守るためにも、使用環境に十分になじませてからお使いください。
- オプションは本体に取り付けられるものであること、また接続できるものであることを確認してください。たとえ本体に取り付けや接続ができても正常に動作しないばかりか、本体が故障することがあります。
- オプションは弊社の純正品をお使いになることをお勧めします。他社製のメモリやハードディスクドライブには本装置に対応したものもありますが、これらの製品が原因となって起きた故障や破損については保証期間中でも有償修理となります。

保守サービスについて

本装置の保守に関して専門的な知識を持つ保守員による定期的な診断・保守サービスを用意しています。
本装置をいつまでもよい状態でお使いになるためにも、保守サービス会社と定期保守サービスを契約されることをお勧めします。

動作保証されない機能について

以下の機能について現時点では動作を保証しておりません。あらかじめご了承ください。

- セーフモードでの起動

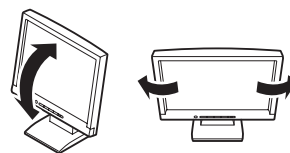
健康を損なわないためのアドバイス

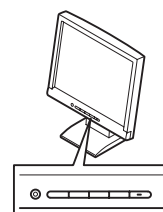
コンピュータ機器を長時間連続して使用すると、身体の各部に異常が起こることがあります。コンピュータを使用するときは、主に次の点に注意して身体に負担がかからないよう心掛けましょう。

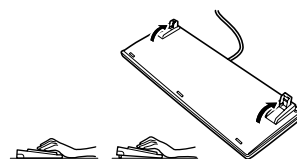
よい作業姿勢で

コンピュータを使用するときの基本的な姿勢は、背筋を伸ばして椅子にすわり、キーボードを両手と床がほぼ平行になるような高さに置き、視線が目の高さよりもやや下向きに画面に注がれているという姿勢です。『よい作業姿勢』とはこの基本的な姿勢をとったとき、身体のどの部分にも余分な力が入っていない、つまり緊張している筋肉がもっとも少ない姿勢のことです。
『悪い作業姿勢』、たとえば背中を丸めたかっこうやディスプレイ装置の画面に顔を近づけたままの状態で作業を行うと、疲労の原因や視力低下の原因となることがあります。

ディスプレイの角度を調節する

ディスプレイの多くは上下、左右の角度調節ができるようになっています。まぶしい光が画面に映り込むのを防いだり、表示内容を見やすくしたりするためにディスプレイの角度を調節することは、たいへん重要です。角度調節をせずに見づらい角度のまま作業を行うと『よい作業姿勢』を保てなくなりすぐに疲労してしまいます。ご使用の前にディスプレイを見やすいよう角度を調整してください。

画面の明るさ・コントラストを調節する

ディスプレイは明るさ(ブライトネス)・コントラストを調節できる機能を持っています。年齢や個人差、まわりの明るさなどによって、画面の最適なブライトネス・コントラストは異なりますので、状況に応じて画面を見やすいように調節してください。画面が明るすぎたり、暗すぎたりすると目に悪影響をもたらします。

キーボードの角度を調節する

オプションのキーボードには、角度を変えることができるよう設計されているものもあります。入力しやすいようにキーボードの角度を変えることは、肩や腕、指への負担を軽減するのにたいへん有効です。

機器の清掃をする

機器をきれいに保つことは、美観の面からだけでなく、機能や安全上の観点からも大切です。特にディスプレイの画面は、ほこりなどで汚れると、表示内容が見にくくなりますので定期的に清掃する必要があります。

疲れたら休む

疲れを感じたら手を休め、軽い体操をするなど、気分転換をはかることをお勧めします。

はじめに

Microsoft® Windows® Embedded Standardを実行するUS300 c を使用することにより、Citrix™ ICAおよびMicrosoft™ RDPセッションサービスを提供するマシンで利用可能なアプリケーション、ファイル、およびネットワークリソースを利用することができます。
US300cの特徴を以下に示します。

- フル機能を搭載したInternet ExplorerブラウザとシンクライアントエミュレーションソフトウェアであるEricom社のPowerTerm® TECがインストールされています。
- ローカルでインストールする各種ソフトウェアによってUS300cのリモート管理を実現し、ローカル保守機能を提供します。
- 32-bit Windows互換のセキュアなWindowsユーザーインタフェースを必要とする環境向けの様々な周辺機器および機能をサポートするアドオンを追加できます。
- Microsoft SilverlightおよびMicrosoft .NET Framework 3.5をサポートしています（SilverlightおよびFrameworkについては、http://www.microsoft.comを参照してください）。

企業ネットワークで可能なセッションサービスやネットワークサービスの利用は、US300 c から企業の仮想プライベートネットワーク（VPN）サーバーに接続して行います。接続方法として以下の方法があります。

- 直接、企業イントラネットに接続する。
- ダイヤル アップサーバーを経由して接続する（企業イントラネット/インターネットに接続）。
- インターネットを経由して接続する（インターネットサービスプロバイダ（ISP）よりインターネットにアクセス）。

本書について

本書は、Microsoft Windows Embedded Standardを実行するUS300ｃの管理者を対象としています。管理者がUS300ｃ環境を設計・管理するために役立つ情報や詳細なシステム設定を紹介しています。

重要 **ご使用のハードウェアまたはソフトウェア構成によっては、表示される画面の内容が本書の例とは異なる場合があります。**

本書は、Microsoft社が提供するMicrosoft Windows Embedded Standardの標準マニュアルを補完するものです。US300ｃを使用することにより生じる差異、強化点、追加機能などを説明しています。

重要 **本書はMicrosoft Windows Embedded Standardの標準機能の説明を意図したものではありません。**

Windows Embedded Standardのヘルプには、マイクロソフトサポートオンラインからアクセスできます（http://support.microsoft.com/default.aspx）。

本書の構成について

本書は以下の章で構成されています。

第1章「US300cについて」では、本製品の設置・接続シャットダウンの方法などについて説明しています。

第2章「サーバー環境の設定」では、Microsoft Windows Embedded Standardを実行するUS300cで、ネットワークサービスやセッションサービスを利用するために必要なネットワークアーキテクチャおよび企業サーバー環境に関する情報を記載しています。また、サーバー環境へのアクセスする際の設定や、サーバー環境が提供するサービスを設定する際に、重要な情報を記載しています。

第3章「導入」では、US300cを使用する際の基本的な設定に役立つ情報を記載しています。US300cの基本機能を説明し、管理者およびユーザー向けにUS300cの設定手順を記述します。

第4章「各種機能の利用」では、コントロールパネルの使用方法、初期設定、ネットワークの設定などについて説明しています。

第5章「応用機能の利用」では、応用機能について説明しています。

第6章「WESの拡張機能の紹介」では、Microsoft Windows Embedded Standardを実行するUS300cの、Windows Embedded Standardに標準装備されていない拡張機能に関する情報を記載しています。

第7章「管理ユーティリティと設定」では、管理に使用するユーティリティおよび設定に関する全般的な情報を記載しています。

第8章「システム管理」では、日常業務の遂行に役立つ、US300c環境をローカルおよびリモートで保守するのに必要なシステムの管理情報を記載しています。

第9章「運用・保守」では、日常の保守、トラブルシューティングについて説明しています。「故障かな？」と思ったときは、装置の故障を疑う前に参照してください。

必要な情報を見つけるには

PDF文書を開いた状態で、[検索]ウィンドウまたは[Find]ツールバー のいずれかを使用して、単語、語句、または単語の一部を検索できます。これらの機能の使用については、ご使用のPDFリーダーのヘルプを参照してください。

付属品の確認

梱包箱の中には、本製品以外にいろいろな付属品が入っています。添付のスタートアップガイドを参照してすべてがそろっていることを確認し、それぞれ点検してください。万一足りないものや損傷しているものがある場合は、販売店に連絡してください。

第三者への譲渡について

本製品を第三者に譲渡(または売却)するときは、本書および添付の部品や説明書、ライセンス許諾書などのドキュメントも一緒にお渡しください。譲渡や売却の際には、必ず渡してください。

消耗品・装置の廃棄について

本製品および電池の廃棄については各自治体の廃棄ルールに従ってください。詳しくは、各自治体へお問い合わせください。なお、本製品に添付の電源コードについても他の装置への転用を防ぐため、本体と一緒に廃棄してください。

本製品の輸送について

本製品およびオプションなどには、リチウム金属電池あるいはリチウムイオン電池を使用しています。リチウム電池の輸送に関しては、航空・海上輸送規制が適用されますので、本製品およびオプションの航空機、船舶等での輸送については、お買い求めの販売店、または保守サービス会社へお問い合わせください。

各種権利、US300cが準拠する規制について

エンドユーザーライセンス契約(「ライセンス」)

Wyse Technology社のエンドユーザーライセンス契約のコピーはソフトウェアに含まれ、参照目的でのみ提供されます。購入日にhttp://www.wyse.com/licenseに掲載されているライセンスが、効力を持つライセンス契約です。ソフトウェアまたは製品をコピー、使用、またはインストールすることによって、ライセンス契約の条件に同意したものとみなします。

限定権利の説明

ユーザーは、本ソフトウェアが米国製であることを確認するものとします。また、ユーザーは、米国輸出管理規則をはじめとする本ソフトウェアに適用されるすべての適用可能な国際法および国内法ならびに米国およびその他の政府によって発行されるエンドユーザー、最終使用、および輸出先国に関する制限事項を遵守するものとします。本ソフトウェアの輸出については、http://www.microsoft.com/exportingを参照してください。

FCC声明

本装置は、テストの結果FCC規則のパート15に従い、クラスAまたはクラスBのデジタルデバイスの制限を遵守していることが確認されています。これらの制限は、住宅に設置するにあたり有害な妨害に対する適切な保護を提供することを目的としています。本装置は無線周波エネルギーを発生、使用、放射しており、指示に従わずに設置または使用された場合、無線通信への有害な妨害の原因となる場合があります。ただし、特定の場所に設置することによって妨害が発生しないという保証はありません。本装置がラジオやテレビの受信の有害な妨害の原因となる場合は(装置電源をオン・オフすることでご確認いただけます)、以下の対策を1つ以上行って妨害を正すことをお勧めします。

- 受信アンテナの向きまたは場所を変更する。
- 装置と受信機の距離をさらに空ける。
- 受信機が接続されているコンセントとは別のコンセントに装置を接続する。
- 取扱店または経験豊富なラジオ技術者またはテレビ技術者に相談する。

本デバイスに適用される関連RF放射制限を確実に遵守するために、本装置にはシールド相互接続ケーブルおよびシールドAC電源ケーブルを使用してください。システムのメーカーによって明示的に許可されていない変更または改造を行うと、装置を操作する権限が無効になる場合があります。

US300cが準拠する規制

基本的なEMCおよび安全要件

US300cは、以下に示されている地域の規制要件に準拠しています。
米国 ― FCC Part 15 (class B), cUL 60950
カナダ ― IC ICES-003, CAN/CSA-C22 No. 60950
ヨーロッパ ― EN 55022 (class B); EN 55024

カナダのDOC通知

クラスA — 本デジタル装置が、カナダ通信省(Department of Communications)の無線妨害規則(Radio Interference Regulations)に定められているデジタル装置からの電波雑音放射について、クラスAの制限を超過することはありません。
Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Réglement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.
クラスB — 本デジタル装置が、カナダ通信省の無線妨害規則に定められているデジタル装置からの電波雑音放射について、クラスBの制限を超過することはありません。
Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe B prescrites dans le Réglement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

ワイヤレスの使用および要件

ワイヤレスオプションを備えたモデルには、無線送信タイプのデバイス(RFモジュール)が含まれています。US300cは、2.4 GHz帯域で動作します(802.11b/g/n WLAN)。
一般的な目安として、US300cの近くでワイヤレスデバイスを使用する場合、ワイヤレスデバイスとUS300cの距離は20 cm(8 inches)程度が一般的です(先端部含まず)。ワイヤレスデバイスが起動し送信中の場合は、本デバイスをから20 cm(8 inches)以上離して使用してください。
状況によっては、ワイヤレスデバイスに関する制限事項が求められる場合があります。一般的な制限事項の例としては、以下のようなものがあります。

- ワイヤレスデバイスを使用した場合の処罰が不明な環境では、ワイヤレスデバイスを使用または電源を入れる前に適切な機関に許可を求めてください。
- ワイヤレスデバイスの使用に関する制限は、国によって異なります。お使いのシステムにはワイヤレスデバイスが装備されていますので、本システムを携帯して国境を越える移動を行う場合は、移動または旅行の前に、行先となる国におけるワイヤレスデバイスの使用に関する制限事項を現地の無線承認機関にご確認ください。
- ワイヤレスデバイスをユーザーが修理することはできません。ワイヤレスデバイスはいかなる方法でも改造しないでください。ワイヤレスデバイスを改造すると、使用許可は無効になります。修理が必要な場合は、メーカーにお問い合わせください。

デバイス電源

発送用のダンボールに含まれている、外部電源モデルPA-1031-0を使用してください。

目　次

5 応用機能の利用 101

6 WESの拡張機能の紹介 117

7 管理ユーティリティと設定 135

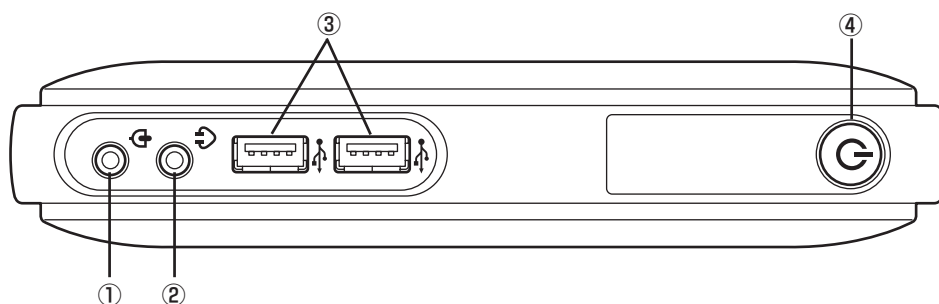
##

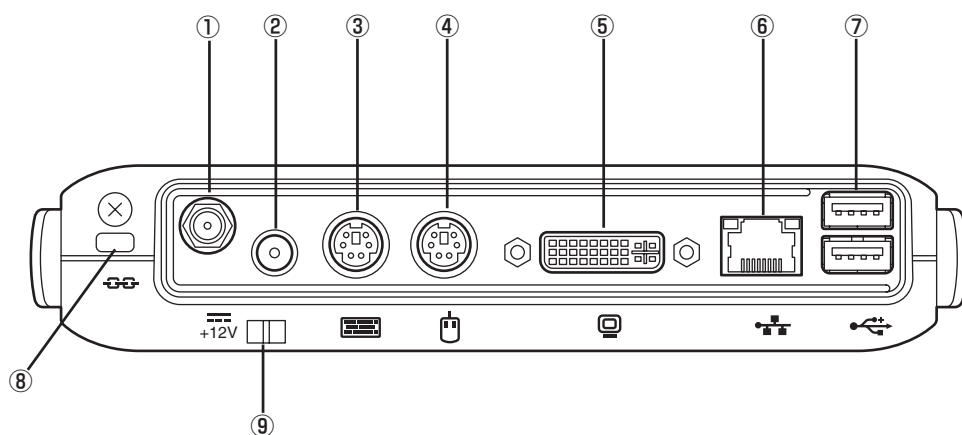
1 US300cについて

本製品の設置、接続、電源をONにする方法などについて説明します。

各部の名称と機能

本製品の各部の名称とその機能を次に示します。

装置前面

① マイクコネクタ(→14ページ)
② ラインアウトコネクタ(→14ページ)
③ USBポート(2箇所)(→14ページ)
④ 電源ボタン

装置背面

① 無線LANアンテナコネクタ

② 電源コネクタ

③ キーボード

④ マウス

⑤ DVIコネクタ

⑥ LANコネクタ

⑦ USBポート

⑧ セキュリティ　スロット

⑨ DC電源コード留め具

- キーボードとマウスを逆に接続しないでください。
  逆に接続するとキーボードやマウスが正常に動作しません。
- DC電源コードは必ず留め具にクランプしてください。

無線LANアンテナ

無線LANアンテナは、本製品に設置されている無線装置からの信号を送信し、受信します。

無線LAN付きモデルに同梱されている無線LANアンテナを、本体の無線LANアンテナポートにしっかりと取り付けてください。
良好な送受信が行えるように、アンテナの向きや角度を調整してください。

本製品に設置されている無線装置は、国際的な指針(ICNIRP)が推奨する無線周波数への露出の限界を超えることがないように設計されています。SAR(特定の吸収率)は、エネルギーが体内組織に吸収される率で、高周波の起点(アンテナ)と人体が離れている距離に強く依存します。
無線装置は、人体とアンテナの距離が、少なくとも2、3cmのときにのみ、無線周波の放出の露出についての国際的な指針に適合します。

USB2.0ポート

4つのUSBポートは、USB規格の周辺機器(例えば、プリンタ、DVDドライブ)を本製品に繋ぐことができます。

USBポートは、たとえシステムの電源が切れているときでも、常時、5Vの電源を外部のUSB装置に供給していますので、外部USB装置はシステムのスイッチを入れずに、いつでもUSB装置に充電することができます。
USB-HUB等の特殊な機能を持つUSBキーボード等の周辺機器を接続した場合、「新しいハードウェアの検出ウィザード」が表示される場合があります。その場合、デバイスドライバをインストールする必要があります。「7章」の「追加ソフトウェアの利用」を参照して接続した周辺機器のデバイスドライバのインストールを行ってください。

AC電源ポート

本製品に、共に同梱されたACアダプタを使用して、AC電源を付け加えます。

本製品と同梱されたACアダプタと2ピンの電源コードだけを使用してください。他のアダプタや電源コードは同じように見えても、それらを使うとシステムを損傷させるおそれがあります。

無線LAN機能

無線LANによって、離れているコンピュータ同士で、データやプログラムなどを共有したり、メッセージを送受信することができます。

使用上の注意

- 通信速度・通信距離は、無線LAN対応機器や電波環境・障害物・設置環境などの周囲条件によって異なります。
- 電波の性質上、通信距離が離れるに従って通信速度は低下する傾向にあります。より快適にお使いいただくために、無線LAN対応機器同士は近い距離で使用することをおすすめします。
- 電子レンジを使用中に無線LAN(IEEE802.11bまたはIEEE802.11gまたはIEEE802.11n)対応機器の通信速度、通信距離が低下する場合があります。無線LAN(IEEE802.11bまたはIEEE802.11gまたはIEEE802.11n)対応機器と電子レンジは離して使用することをおすすめします。
- 無線LAN(IEEE802.11bまたはIEEE802.11gまたはIEEE802.11n)対応機器とBluetooth™対応機器を同時に使用された場合、それぞれの機器の通信速度や通信距離が低下する場合があります。無線LAN(IEEE802.11bまたはIEEE802.11gまたはIEEE802.11n)対応機器とBluetooth™対応機器はいずれかをオフにするか、離して使用することをおすすめします。
- ネットワークへの接続には、別売の無線LANアクセスポイント(以下アクセスポイント)などが必要です。
- 医療機関側が本製品の使用を禁止した区域では、本製品の電源を切るか無線LAN機能をオフにしてください。また、医療機関側が本製品の使用を認めた区域でも、近くで医療機器が使用されている場合には、本製品の電源を切るか無線LAN機能をオフにしてください。
- ネットワークとの通信中は、本製品を休止状態やスタンバイ状態にしないでください。
- スタンバイ状態または休止状態では、ネットワーク機能がいったん停止しますので、ファイルコピー等の通信動作が終了してからスタンバイ状態または休止状態にしてください。また、使用するアプリケーションによっては、スタンバイ状態または休止状態から復帰した際にデータが失われることがあります。ネットワークを使用するアプリケーションを使う場合には、あらかじめお使いのアプリケーションについてシステム管理者に確認のうえ、スタンバイ状態または休止状態を使用してください。

無線LAN製品ご使用時におけるセキュリティに関するご注意

無線LANでは、LANケーブルを使用するかわりに、電波を利用してパソコン等と無線アクセスポイント間での情報のやりとりを行うため、電波の届く範囲であれば自由にLAN接続が可能であるという利点があります。

その反面、電波はある範囲内であれば障害物（壁等）を超えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

- 通信内容を盗み見られる

  悪意ある第三者が、電波を故意に傍受し、

  - IDやパスワードまたはクレジットカード番号等の個人情報
  - メールの内容

  等の通信内容を盗み見られる可能性があります。

- 不正に侵入される

  悪意ある第三者、無断で個人や会社内のネットワークへアクセスし、

  - 個人情報や機密情報を取り出す（情報漏洩）
  - 特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
  - 傍受した通信内容を書き換えて発信する（改ざん）
  - コンピュータウイルスなどの流しデータやシステムを破壊する（破壊）

  などの行為をされてしまう可能性があります。

本来、無線LANカードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線LAN製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。

セキュリティの設定を行わないで使用した場合の問題を十分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをおすすめします。

セキュリティの設定などについて、お客様ご自身で対処できない場合には、ファーストコンタクトセンターまでお問い合わせください。

セキュリティ対策を施さず、あるいは、無線LANの仕様上やむを得ない事情によりセキュリティの問題が発生してしまった場合、弊社はこれによって生じた損害に対する責任を負いかねます。

本機で設定できるセキュリティ

- 次のセキュリティについての設定をする場合、使用するアクセスポイントなどもこれらの設定に対応している必要があります。
- これらの設定は危険性をより低くするための手段であり、安全性を100%保証するものではありません。

盗聴(傍受)を防ぐ

本製品の無線LAN機能は「WEP(Wired Equivalent Privacy)機能」に対応しています。WEP機能を使用して暗号キーを設定すると、同じ暗号キーを使用している通信機器間の無線LANの通信データを暗号化できるので、通信を盗聴されたり、関係のないパソコンや機器との接続を防ぐことができます。WEP機能には64ビットWEP対応、128ビットWEP対応、152ビットWEP対応のものがあり、本製品の無線LAN機能は、すべてに対応しています。
ただし、暗号キーを設定していても、暗号キー自体を第三者に知られたり、暗号解読技術によって暗号を解読されたりする可能性があるため、設定した暗号キーは定期的に変更することをおすすめします。

WEP機能を利用するには、通信する相手の機器もWEP機能に対応している必要があります。

不正アクセスを防ぐ

- アクセスポイントと通信機器の両方に任意のSSID(ネットワーク名)を設定することで、同じSSIDを設定していない通信機器からの接続を回避できます。ただし、第三者にSSIDを自動的に検出する機能を持った機器を使用されると、SSIDを知られてしまいます。これを回避するには、アクセスポイント側でSSIDを通知しないように、SSIDの隠蔽の設定をする必要があります。
- 接続するパソコンなどのMACアドレス(ネットワークカードが持っている固有の番号)をアクセスポイントに登録することで、登録した機器以外はアクセスポイントに接続できなくなります(MACアドレスフィルタリング)。

より高度なセキュリティ設定を行う

Wi-Fi Allianceが提唱するWPA(Wi-Fi Protected Access)機能を利用します。
IEEE802.1X/EAP(Extensible Authentication Protocol)規格によるユーザ認証、従来のWEP機能に比べて大幅に暗号解読が困難とされる暗号方式 TKIP(Temporal Key Integrity Protocol)やAES(Advanced Encryption Standard)を使用することで、より高度なセキュリティ設定を行うことができます。

WPAによる暗号化を使用するためには、接続する相手の機器も同じセキュリティ機能に対応している必要があります。

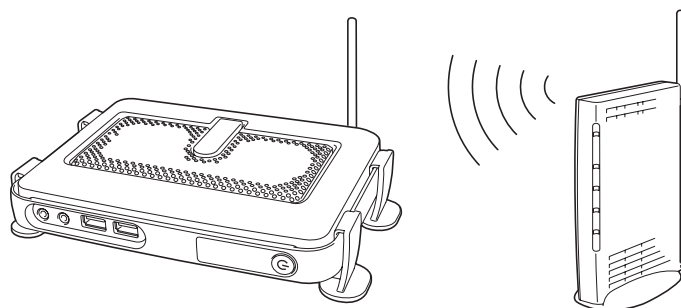
無線LANの設定

本書の「ワイヤレスネットワーク接続」(88ページ)をご覧になり、設定を行ってください。

無線LAN機能でできること

本製品の無線LAN機能を使用することで、次のようなことができます。

無線LAN対応周辺機器（親機）との無線接続

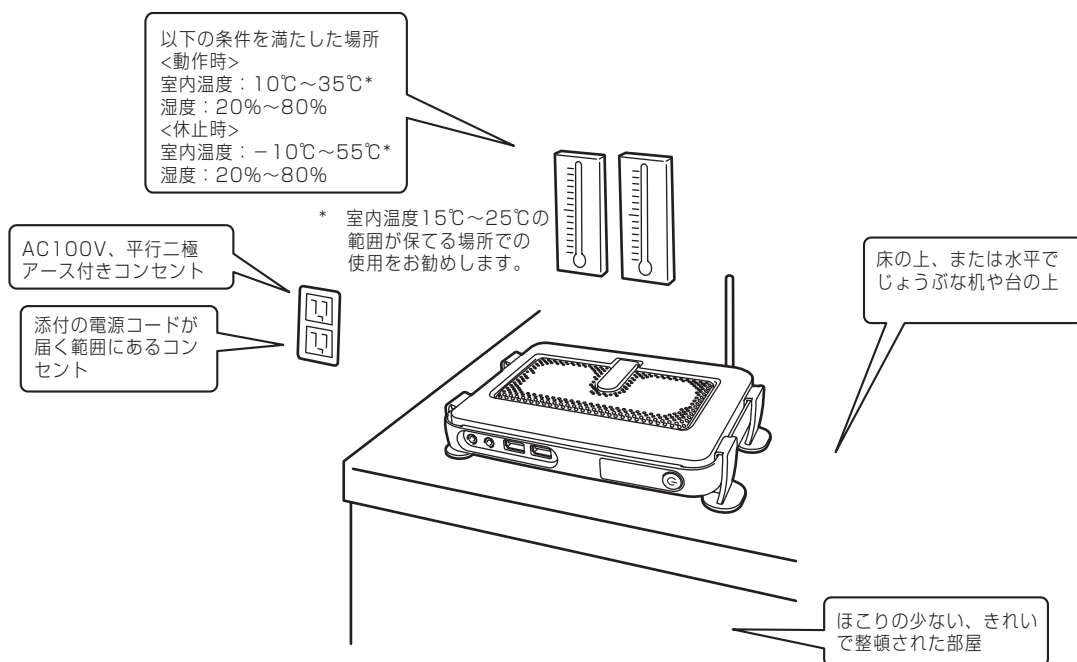
本製品と無線LANに対応した別売の周辺機器（親機）を使用すると、ケーブルで接続せずにLANを利用することができます。例えば、無線LANに対応したルータやターミナルアダプタなどを利用してインターネットに接続することができます。

設置

本製品の設置の方法について以下に説明します。

設置

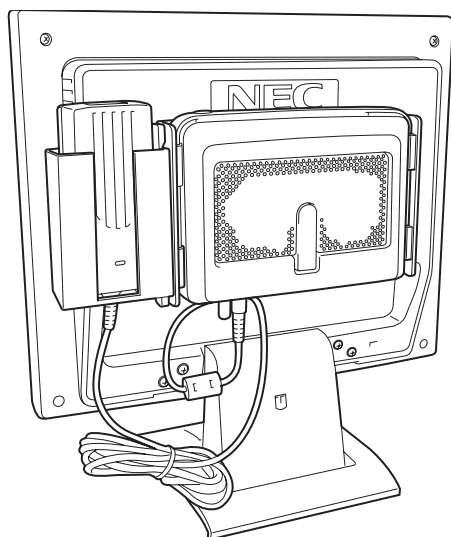
本製品を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- 指定以外の場所に設置しない

設置にふさわしい場所は次のとおりです。

次に示す条件に当てはまるような場所には、本製品を設置しないでください。これらの場所に本製品を設置すると、誤動作の原因となります。

- 温度変化の激しい場所(暖房器、エアコン、冷蔵庫などの近く)。
- 強い振動の発生する場所。
- 腐食性ガスの発生する場所(大気中に硫黄の蒸気が発生する環境下など)、薬品類の近くや薬品類がかかるおそれのある場所。
- 帯電防止加工が施されていないじゅうたんを敷いた場所。
- 物の落下が考えられる場所。
- 電源コードまたはインタフェースケーブルを足で踏んだり、引っ掛けたりするおそれのある場所。
- 強い磁界を発生させるもの(テレビ、ラジオ、放送/通信用アンテナ、送電線、電磁クレーンなど)の近く(やむを得ない場合は、保守サービス会社に連絡してシールド工事などを行ってください)。
- 本体の電源コードを他の接地線(特に大電力を消費する装置など)と共用しているコンセントに接続しなければならない場所。
- 電源ノイズ(商用電源をリレーなどでON/OFFする場合の接点スパークなど)を発生する装置の近くには設置しないでください。(電源ノイズを発生する装置の近くに設置するときは電源配線の分離やノイズフィルタの取り付けなどを保守サービス会社に連絡して行ってください。)

N8120−106 LCD取り付けブラケット(オプション)を使用した設置

N8120-106 LCD取り付けブラケットを使用した設置方法の詳細については、
N8120-106 LCD取り付けブラケットに添付の取扱説明書をご覧ください。

LCD取り付けブラケットを使用して本製品をLCD背面に設置した場合

DC電源コードは必ず留め具にクランプしてください。

接続

本製品をネットワークに接続します。
ネットワークケーブルを接続してから添付のACアダプタの電源コードを本製品に接続し、電源プラグをコンセントに接続します。

⚠ 警告

本製品を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

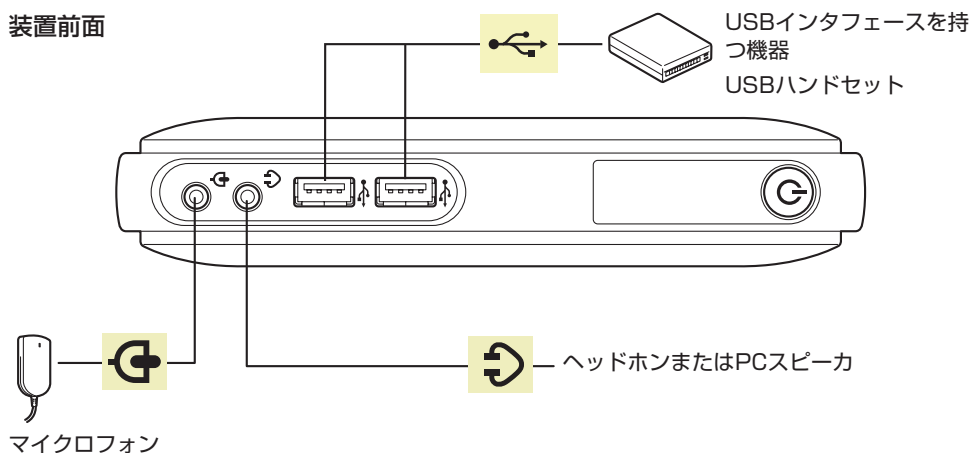
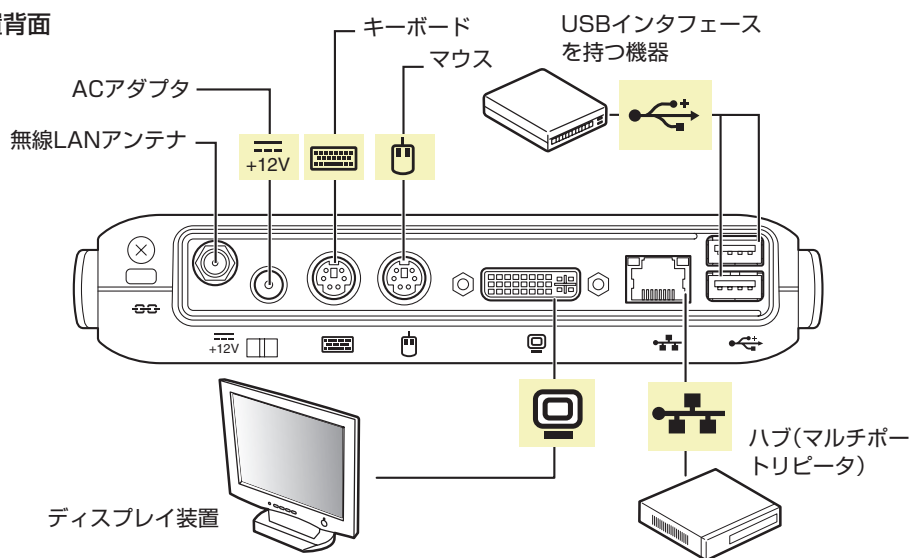
- ぬれた手で電源プラグを持たない

⚠ 注意

本製品を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- 指定以外のコンセントに差し込まない
- たこ足配線にしない
- 中途半端に差し込まない
- 指定以外の電源コードを使わない
- プラグを差し込んだままインタフェースケーブルの取り付けや取り外しをしない
- 指定以外のインタフェースケーブルを使用しない

重要

- 本製品および接続する周辺機器の電源をOFFにしてから接続してください。ONの状態のまま接続すると誤動作や故障の原因となります。
- サードパーティの周辺機器およびインタフェースケーブルを接続する場合は、お買い求めの販売店でそれらの装置が本製品で使用できることをあらかじめ確認してください。サードパーティの装置の中には本製品で使用できないものがあります。サードパーティの周辺機器、またはNECが認定していない装置やインタフェースケーブルを使用したために起きた本製品の故障については、その責任を負いかねますのでご了承ください。
- LANコネクタに接続したケーブルを抜くときは、コネクタのツメが手では押しにくくなっているため、マイナスドライバなどを使用してツメを押して抜いてください。その際に、マイナスドライバなどがLANコネクタやその他のコネクタを破損しないよう十分に注意してください。

システムBIOSのセットアップ

Basic Input Output System(BIOS)の設定方法について説明します。

本製品を導入したときやオプションの増設/取り外しをするときはここで説明する内容をよく理解して、正しく設定してください。

概要

SETUPはハードウェアに基本設定をするためのユーティリティツールです。このユーティリティは本体内のフラッシュメモリに標準でインストールされているため、専用のユーティリティなどがなくても実行できます。

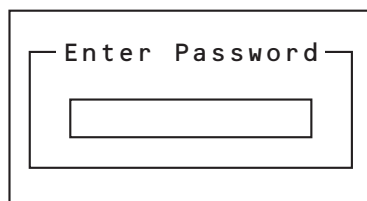
SETUPで設定される内容は、出荷時に最も標準で最適な状態に設定していますのでほとんどの場合においてSETUPを使用する必要はありませんが、この後に説明するような場合など必要に応じて使用してください。

重要

- SETUPの操作は、システム管理者(アドミニストレータ)が行ってください。
- SETUPでは、パスワードを設定することができます。
- 初期パスワードは“Fireport”(大文字・小文字区別)です。
- SETUPは、最新のバージョンがインストールされています。このため設定画面が本書で説明している内容と異なる場合があります。設定項目については、オンラインヘルプを参照するか、保守サービス会社に問い合わせてください。
- SETUPはExitメニューまたは<Esc>、<F10>キーで必ず終了してください。
SETUPを起動した状態でパワーオフ、リセットを行った場合にはSETUPの設定が正しく更新されないことがあります。

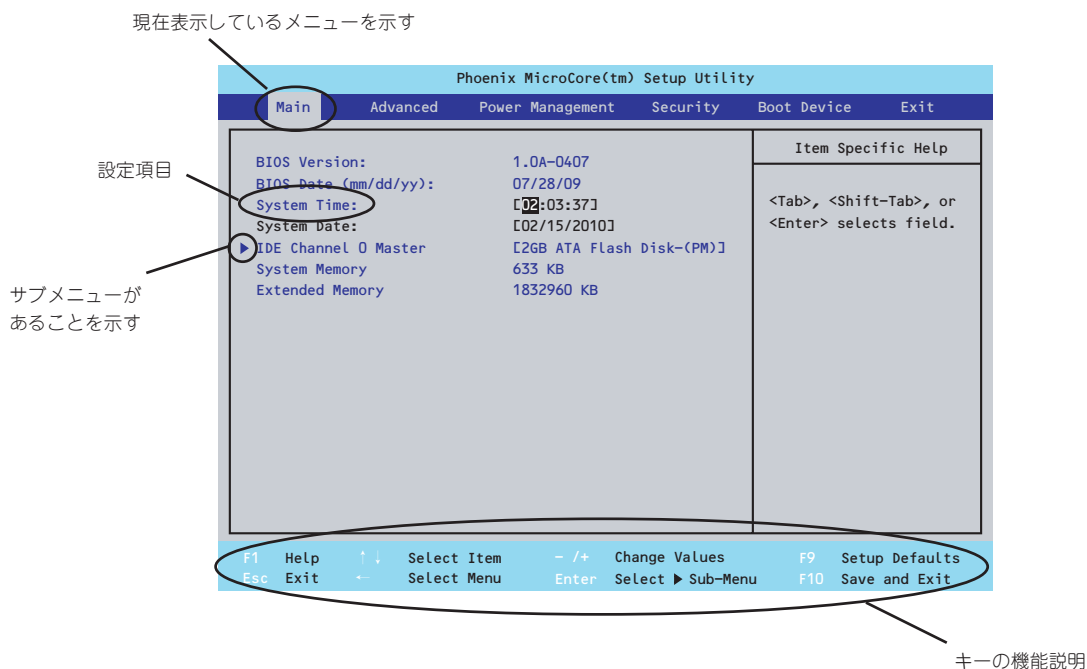
起動

本製品の電源をONにしてBIOS診断画面が短い時間表示されます。この表示中に<Del>キーを押すと、SETUPが起動してMainメニュー画面を表示します。

SETUPメニューを初めて起動するとき、もしくは、以前にSETUPを起動してパスワードの変更をしている場合は、パスワードを入力する画面が表示されます。パスワードを入力してください。
初めて起動するときのパスワードは“Fireport”(大文字・小文字区別)です

パスワードの入力は、3回まで行えます。3回とも誤ったパスワードを入力すると、本製品は動作を停止します(これより先の操作を行うことができません)。電源をOFFにしてください。パスワードを3回間違えてもBIOSはロックされません。再度電源をONにしてSETUPの起動からやり直してください。

BIOS診断画面がエラーでストップした場合は、＜Del＞キーを押して一度SETUPメニューを起動してください。
BIOS診断画面がエラーでストップした場合は、＜F1＞キーを押さないでください、BIOS SETUPメニューの設定が初期値に戻ります。

キーと画面の説明

キーボード上の次のキーを使ってSETUPを操作します(キーの機能については、画面下にも表示されています)。

キー	説明
カーソルキー(←、→)	Main,Advanced,Power Management, Security, Boot Device, Exitなどのメニューを選択します。
カーソルキー(↑、↓)	画面に表示されている項目を選択します。文字の表示が反転している項目が現在選択されています。
<+>キー/<->キー	選択している項目の値(パラメータ)を変更します。サブメニューを選択している場合、このキーは無効です。
<+>キー	選択している項目の現在の設定値をひとつ次の設定値に変更します(増加)。
<->キー	選択している項目の現在の設定値をひとつ前の設定値に変更します(減少)。
<F1>キー	SETUP画面内のキー操作のヘルプを表示します。
<F9>キー	すべての設定値にデフォルト値を書き込みます
<F10>キー	設定したパラメータを保存してSETUPを終了します。
<Esc>キー	一つ前の画面に戻ります。押し続けると「Exit」メニューに進みます。
<Enter>	サブメニューの選択をします。

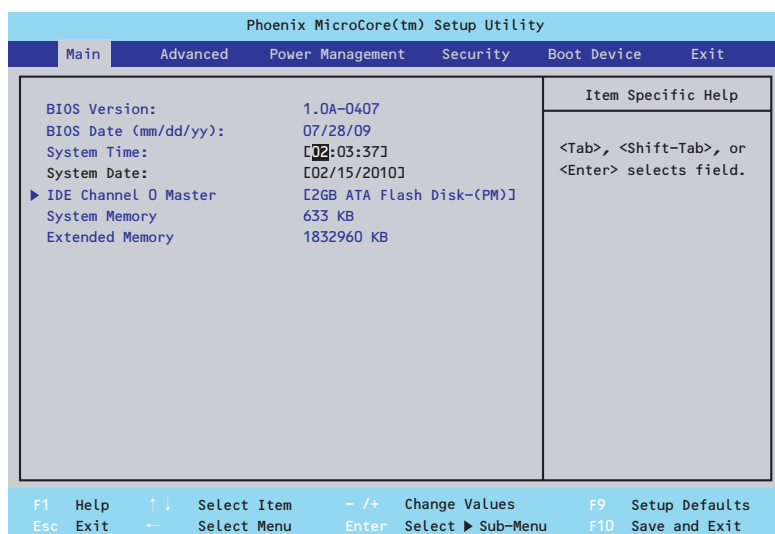
パラメータと説明

Setupには大きく6種類のメニューがあります。

- Mainメニュー
- Advancedメニュー
- Power Managementメニュー
- Securityメニュー
- Boot Deviceメニュー
- Exitメニュー

このメニューの中からサブメニューを選択することによって、さらに詳細な機能表示ができます。次に画面に表示されるメニュー別に設定できる機能やパラメータ、出荷時の設定を説明します。

Main

SETUPを起動すると、はじめにMainメニューが表示されます。
項目の前に「▶ 」が付いているメニューは、選択して「Enter」を押すと、サブメニューが表示されます。

Mainメニューの画面上で設定できる項目とその機能を示します。
項目については次の表を参照してください。

項　目	パラメータ	説　明
System Time	HH:MM:SS	時刻の設定をします。
System Date	MM/DD/YYYY	日付の設定をします。
IDE Channel 0 Master	―	IDEの情報を確認します。

BIOSのパラメータで時刻や日付の設定が正しく設定されていることを必ず確認してください。次の条件に当てはまる場合は、運用の前にシステム時計の確認・調整を行ってください。

- 装置の輸送後
- 装置の保管後

システム時計は、毎月1回程度の割合で確認してください。
システム時刻を調整しても時間の経過と共に著しい遅れや進みが生じる場合は、お買い求めの販売店、または保守サービス会社に保守を依頼してください。

IDE Channel 0 Master

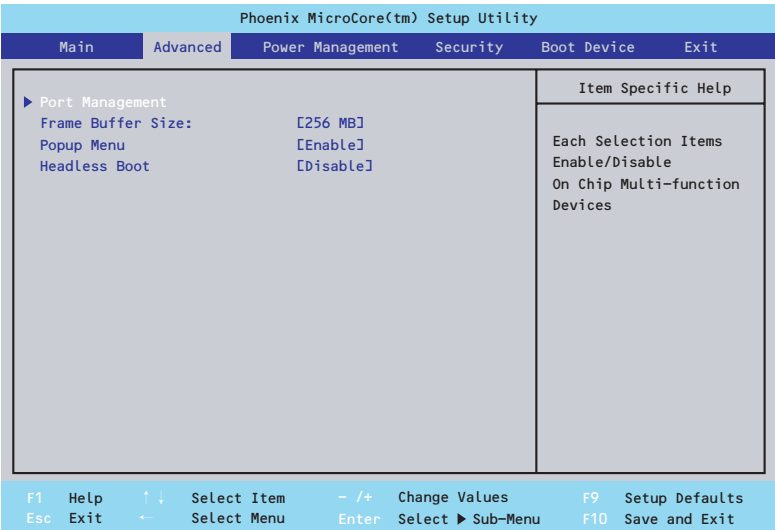
Mainメニューで「IDE Channel 0 Master」を選択すると、IDEの情報を確認できます。

IDE Channel 0 Masterメニューの画面上で設定できる項目とその機能を示します。
項目については次の表を参照してください。

項　目	パラメータ	説　明
Type	[Auto] User Other ATAPI CD-ROM IDE Removable ATAPI Removable None	設定変更しないでください。
32 Bit I/O	Enable [Disable]	設定変更しないでください。

パラメータ欄の[　]はBIOSデフォルト値になります。

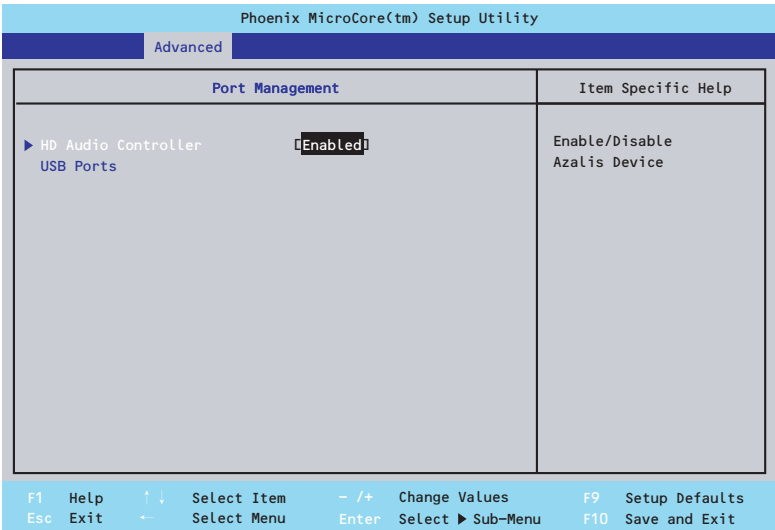
Advanced

カーソルを「Advanced」の位置に移動させると、Advancedメニューが表示されます。

Advancedメニューの画面上で設定できる項目とその機能を示します。
項目については次の表を参照してください。

項　目	パラメータ	説　明
Port Management	―	各ポートの設定を確認します。
Frame Buffer Size	64M 128M [256M] 512M	グラフィックのメモリサイズの設定をします。
Popup Menu	[Enable] Disable	設定変更しないでください。
Headless Boot	Enable [Disable]	設定変更しないでください。

パラメータ欄の[　]はBIOSデフォルト値になります。

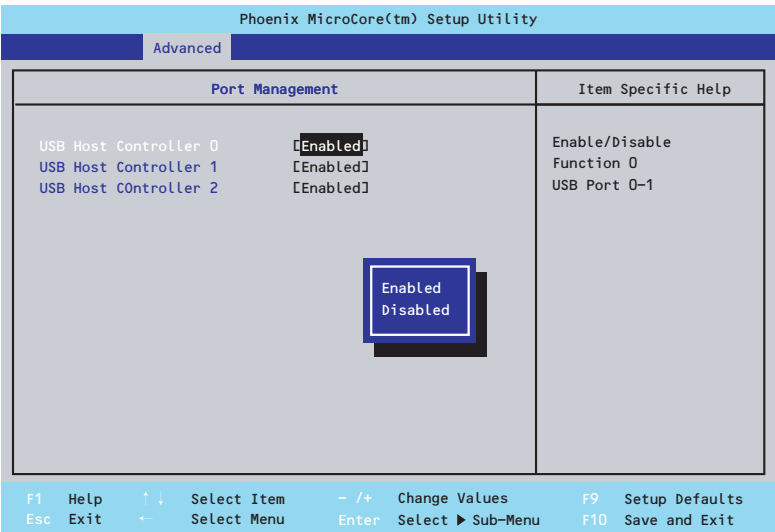
Port Management

Advancedメニューで「Port Management」を選択すると、各ポートの設定を確認できます。

Port Managementメニューの画面上で設定できる項目とその機能を示します。
項目については次の表を参照してください。

項　目	パラメータ	説　明
HD Audio Controller	[Enable] Disable	Audioのサポートを有効/無効にします。
USB Ports	—	USBポートの設定を確認します。

パラメータ欄の[　]はBIOSデフォルト値になります。

USB Ports

Port Managementメニューで「USB Ports」を選択すると、USBポートの設定を確認できます。

USB Portsメニューの画面上で設定できる項目とその機能を示します。
項目については次の表を参照してください。

項　目	パラメータ	説　明
USB Host Controller 0	[Enable] Disable	USB Host Controller 0サポートを有効/無効にします。 ただし、無効にした場合は、USB Host Controller 1と2も無効になります。
USB Host Controller 1	[Enable] Disable	USB Host Controller 1サポートを有効/無効にします。
USB Host Controller 2	[Enable] Disable	USB Host Controller 2サポートを有効/無効にします。

パラメータ欄の[　]はBIOSデフォルト値になります。

Power Management

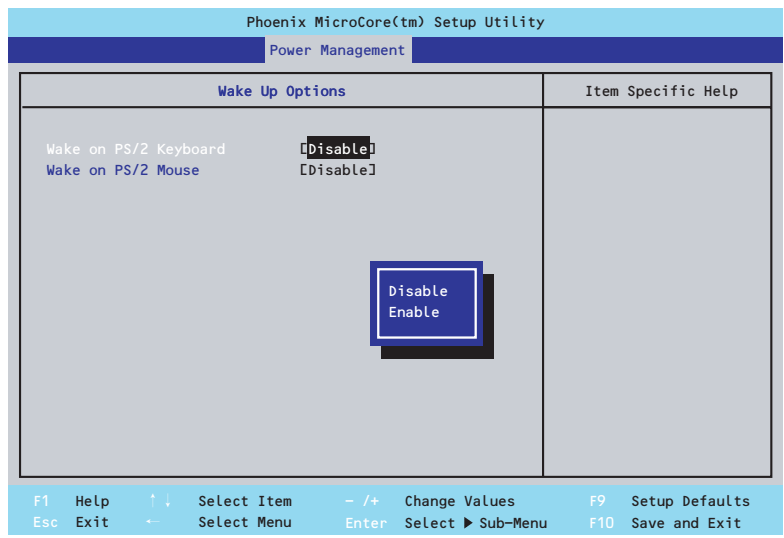
カーソルを「Power Management」の位置に移動させると、Power Managementメニューが表示されます。

Power Managementメニューの画面上で設定できる項目とその機能を示します。
項目については次の表を参照してください。

項　目	パラメータ	説　明
Power States	Always On Last State [Off]	ACアダプタからのAC電源が失われ、再度AC電源を入れた時、どの状態に復旧するかを設定します。 「Off」に設定すると、ACアダプタのAC電源投入時に本機のDC電源は入りません。 「Last State」に設定すると、ACアダプタのAC電源が失われた時の状態に戻します。DC電源が入っている状態でACアダプタのAC電源が切れた場合は、DC電源が入ります。DC電源が切れている状態でACアダプタのAC電源が切れた場合は、DC電源は入りません。 「Always ON」に設定すると、ACアダプタのAC電源投入時に本機のDC電源が入ります。
Wake Up Options	－	デバイスからのWakeup設定を確認します。

パラメータ欄の[　]はBIOSデフォルト値になります。

Wake Up Options

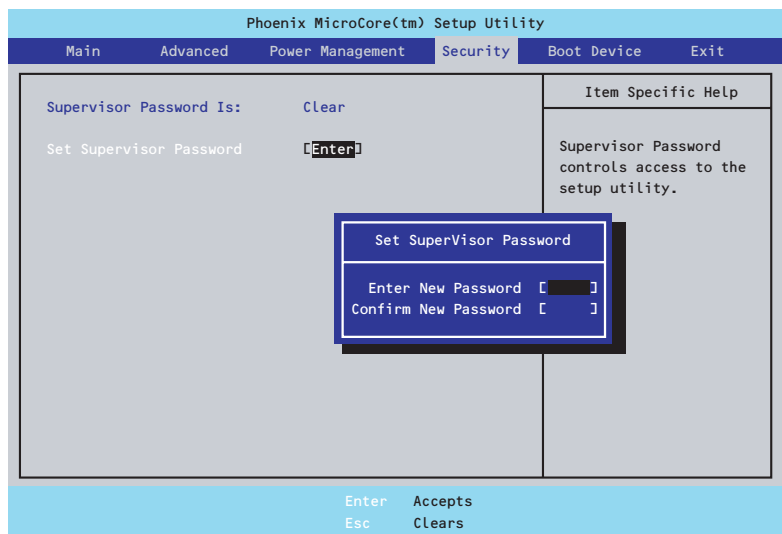
Power Managementメニューで「Wake Up Options」を選択すると、デバイスからのWakeup設定を確認できます。

Wake Up Optionsメニューの画面上で設定できる項目とその機能を示します。
項目については次の表を参照してください。

項　目	パラメータ	説　明
Wake on PS/2 Keyboard	Enable [Disable]	設定変更しないでください。
Wake on PS/2 Mouse	Enable [Disable]	設定変更しないでください。

パラメータ欄の[　]はBIOSデフォルト値になります。

装置がスリープ状態の時に、キーボードやマウスを操作するとWakeupします。

Security

カーソルを「Security」の位置に移動させると、Securityメニューが表示されます。

Securityメニューの画面上で設定できる項目とその機能を示します。
項目については次の表を参照してください。

項　目	パラメータ	説　明
Supervisor Password IS	Clear [Set]	パスワードの設定状態を示します。
Set Supervisor Password		初期パスワードは “Fireport” です。 (大文字/小文字は区別します)

パラメータ欄の[ ] はBIOSデフォルト値になります。

Boot Device

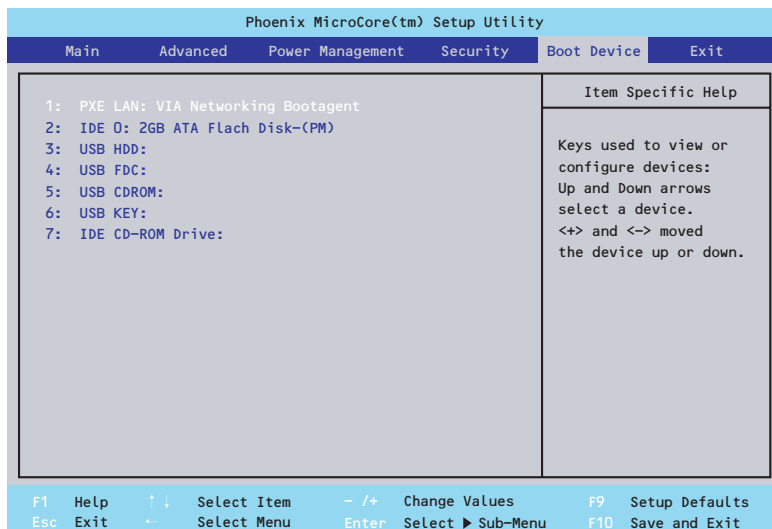
カーソルを「Boot Device」の位置に移動させると、Boot Deviceメニューが表示されます。

起動するデバイスを優先順に従ってリスト表示します。先頭デバイスからオペレーティングシステムを起動します。もしもオペレーティングシステムが存在しないなど起動に失敗した場合は次のデバイスから起動します。

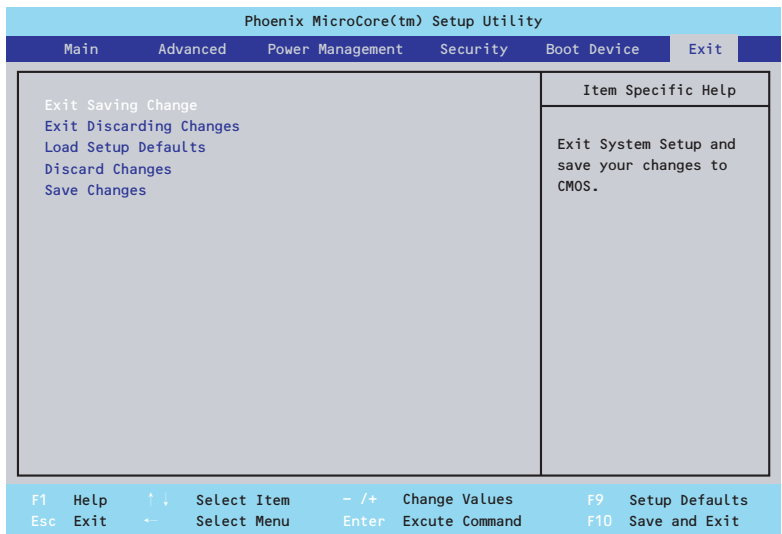
起動するデバイスを変更するには<↑><↓>キーを使用して変更したいデバイスにカーソルを合わせます。
<+>キーを押すとリストの上側に移動し、<->キーを押すとリストの下側に移動します。

出荷時の設定は、以下の優先順位に設定されています。

1. ON Board LANデバイス
2. マスターハードディスク
3. USB HDD デバイス
4. USB FDCデバイス
5. USB CD-ROMデバイス
6. USB KEYデバイス
7. IDE CD-ROMデバイス

実際の画面には、以下のように表示されます。

IDE CD-ROM Driveは未サポートです。

Exit

カーソルを「Exit」の位置に移動させると、Exitメニューが表示されます。

このメニューの各オプションについて説明します。

設定項目	説　明
Exit Saving Change	変更した内容を保存し BIOS セットアップメニューを終了します。 （<F10>キーを押す終了方法と同じとなります。）
Exit Discarding Changes	設定値を保存せずに（現在設定した値を破棄して）、BIOS セットアップメニューを終了します。
Load Setup Defaults	すべての設定値にデフォルト値を書き込みます。 ここでの「デフォルト値」は、工場出荷時の値とは異なる場合があります。
Discard Changes	変更前の値に戻します。 （BIOS セットアップメニューは継続されます。）
Save Change	変更した値を保存します。 （BIOS セットアップメニューは継続されます。）

US300cの利用

US300cのシステム構成、基本的な操作方法、仮想PCへの接続方法、シャットダウンの方法などについて以下に説明します。

ここに記載するシステム構成では、ハブ、ルータ等のネットワーク機器の記載は省略しています。

US300cは、仮想PCに接続するシンクライアント装置です。
シンクライアントシステムの最小構成は、US300cと仮想PCをホストするサーバーのみで構成できます(1.基本構成)。
基本構成を拡張して、DHCPサーバー、WDM(Wyse Device Manager)サーバー、ダウンロードサーバー(FTPサーバー)を利用して、シンクライアントシステムの保守性を向上させることができます(2. 拡張1)。
拡張構成として、VPCCの管理ツール(SSC)を使用することもできます(3. 拡張3)。
仮想PCに接続するネットワーク環境としてVPNを使用することもできます(4. VPN)。

1. 基本構成

シンクライアントシステムの最小構成は、US300cと仮想PCをホストするサーバーのみで構成できます。US300cの初期設定として、ネットワークの設定を行い、リモートデスクトップ接続で仮想PCの接続先を設定すれば、仮想PCに接続できます。

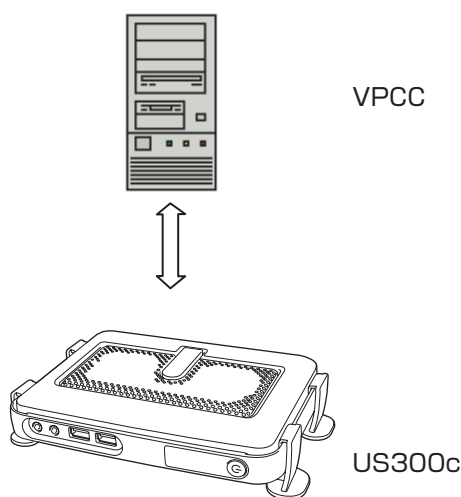



図1-1　基本構成

● **VPCC(Virtual PC Center)**

仮想PCをホストするサーバーです。仮想PCとして、Windows XP Professional、Windows Vista Business、Enterprise Edition、Windows 7 Enterprise Edition をホストします。

US300cはVPCC以外にも、Windows Server 2003、Windows Server 2008、Citrix XenApp(Presentation Server 4.5)への接続をサポートします。

2. 拡張1

基本構成を拡張して、DHCPサーバー、WDMサーバー、ダウンロードサーバ(FTPサーバー)を利用して、シンクライアントシステムの保守性を向上させることができます。DHCPを使用するネットワークでは、US300c用にDHCPオプション情報を設定して、WDMサーバーの情報を取得し、WDMサーバーからUS300cを一括管理することができます。US300cの時刻をサーバーと合わせるようにするにはインターネット時刻サーバーを使用します。

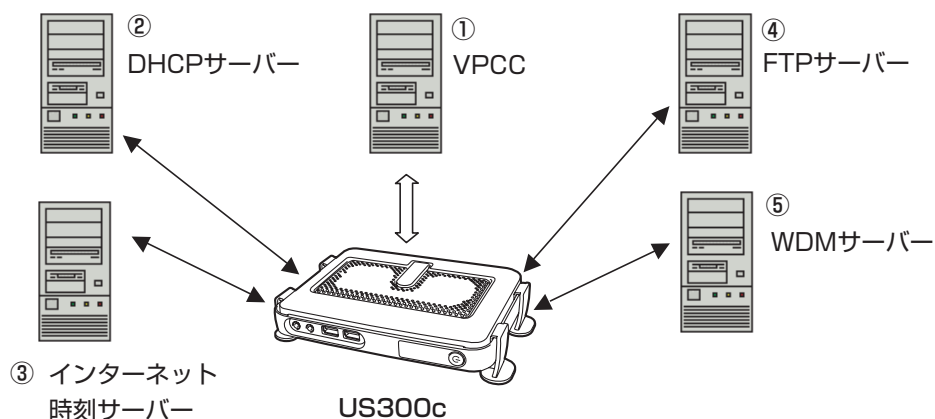



図1-2　拡張1

① VPCC(Virtual PC Center)

② DHCPサーバー

US300cのIPアドレスや他の情報をDHCPサーバーから取得します。ダウンロードサーバーの情報をDHCPサーバーから取得することもできます。

③ インターネット時刻サーバー

US300cにインターネット時刻サーバーの設定を行うと、起動時にインターネット時刻サーバーと時刻同期します。

④ FTPサーバー(ダウンロードサーバー)

FTP Addon Installerを使用する際に、アプリケーション(MSI形式)をFTPサーバーからダウンロードしてUS300cにインストールすることができます。

⑤ WDMサーバー

アップデートモジュール、アプリケーション等のUS300cへの配信、設定変更等、US300cをリモートで管理することができます。

3.　拡張2

US300cと、VPCCの管理ツール(SSC)と連携して、シンクライアントシステムの保守性を向上させることができます。US300cでは、SSCと連携する機能として、クライアント管理オプション(CMO)に対応します。

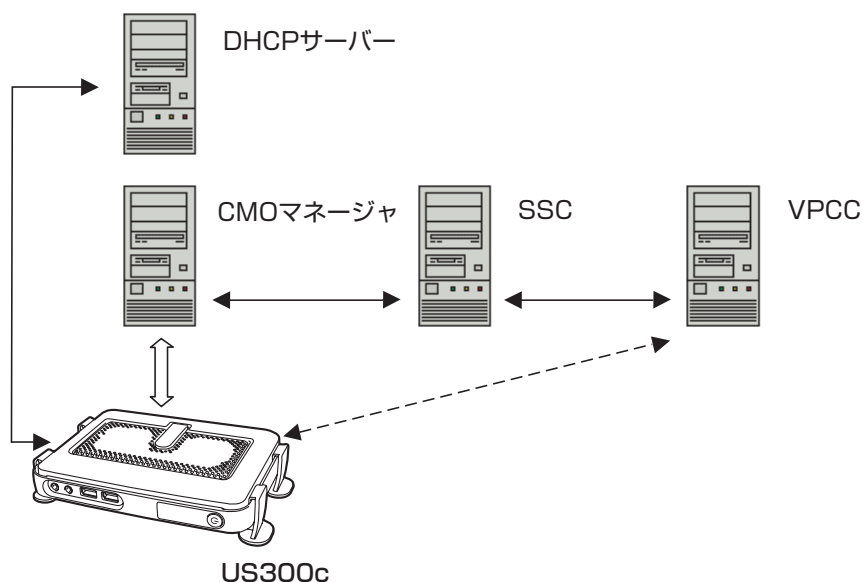



図1-3　拡張2

- **VPCC(Virtual PC Center)**
- **DHCPサーバー**

  US300cのIPアドレスや他の情報をDHCPサーバーから取得します。DHCPオプションを使用すると、CMOマネージャのサーバーアドレスを自動で取得するようにUS300cを設定できます。

- **SSC**

  VPCCで動作する仮想PCを管理するサーバーです。CMOマネージャがSSCと連携して動作します。

- **CMOマネージャ**

  クライアント管理オプションのサーバー機能です。US300cから接続する仮想PCの接続先情報を一元管理します。クライアント管理オプションを使用すると、ユーザはUS300c上で使用できる仮想PCの一覧から選択して、仮想PCに接続することができます。

4. VPN

仮想PCに接続するネットワーク環境としてVPNを使用することができます。

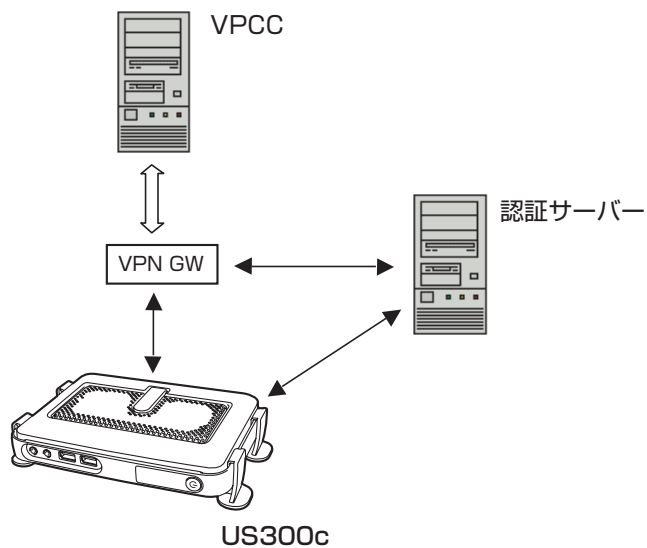



図1-4　VPN

- **VPCC(Virtual PC Center)**
- **VPN GW**

  US300cでは、VPNのプロトコルとしてL2TPが使用できます。US300cを接続するVPNゲートウェイにてL2TPを設定してください。
- **認証サーバー**

  VPN GWからの認証要求に応答して、接続ユーザの認証を行います。US300cでは、認証サーバーに送信するアカウントの入力を行います。

US300cの基本的な操作方法

US300cは仮想PCに接続するためのシンクライアントとして、US300cに関する設定、操作をできるだけ少なくするように設計しています。

US300cでは、「スタート」メニューから仮想PCへの接続プログラムと、コントロールパネルのツールを起動することで基本的な操作を行います。

- US300cの電源をONにすると、デスクトップ画面が表示されます。「スタート」メニューから仮想PCへの接続、コントロールパネルのツールの起動、US300cのシャットダウンを行うことができます。
- 仮想PCに接続するために「スタート」メニューからリモートデスクトップ接続を起動することができます。
- US300cの設定を変更するには、コントロールパネルのツールを使用します。「スタート」メニューから起動します。
- US300cの電源をOFFにするときは、「スタート」メニューからシャットダウンを行います。

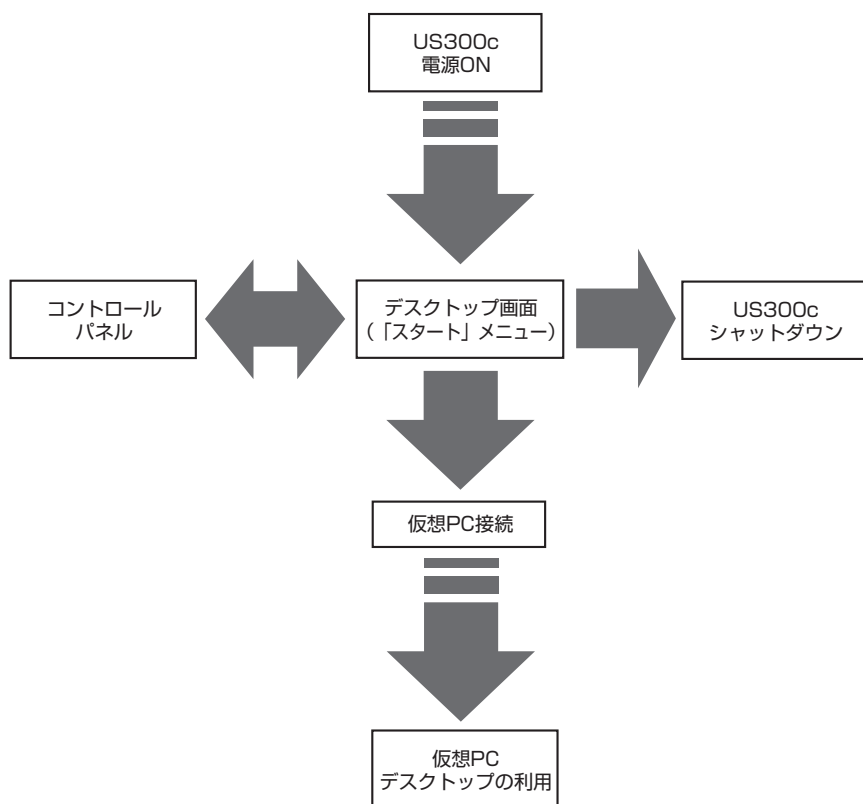



図1-5　US300cの基本操作

US300cでは、仮想PCへの接続にリモートデスクトップ接続を使用します。リモートデスクトップ接続は、仮想PCのコンピュータ名を入力するだけで、仮想PCへの接続に利用できます。システム管理者から割り当てられた仮想PCのアドレスをコンピュータ名に設定して接続を開始してください。

US300cの設定を変更するにはコントロールパネルを使用します。コントロールパネルは、「スタート」メニューから開くことができます。

US300cは、使い始めるために必要な操作を少なくすることで、シンクライアントシステムをわかりやすく操作して頂くことを目指しています。

日付と時刻を設定する

US300cの日付と時刻はコントロールパネルから設定することができます。

図1-6　日付と時刻

1. 「スタート」メニューから「コントロールパネル」を選択し、「日付と時刻」を起動する。
2. 「日付と時刻のプロパティ」にて、日付と時刻を設定する。
3. 必要な場合は、タイムゾーンを設定する。
   タイムサーバーを利用する場合はインターネット時刻を設定してください。
4. 設定が終わったら「OK」ボタンを押下する。

現在の日付とUS300cのシステムの日付に大きな差異がある時に、インターネット時刻サーバーとの時刻同期に失敗する事があります。失敗が発生する場合は、システムの日付を手動で現在の日付に合わせて頂いた後インターネット時刻サーバーとの時刻同期を行ってください。

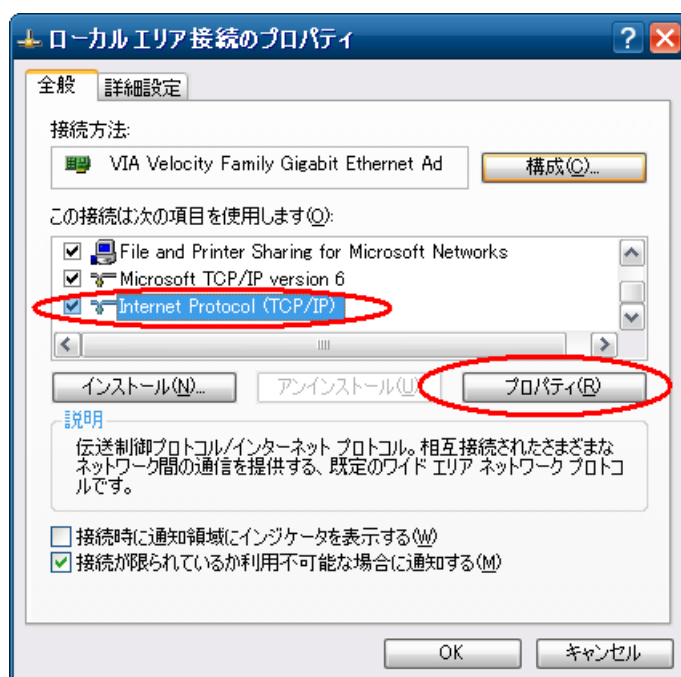
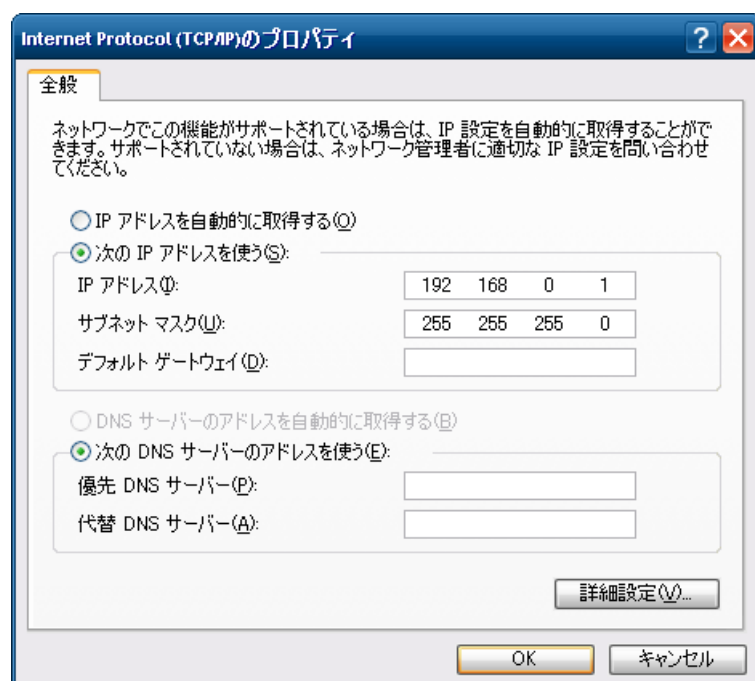
ネットワークを設定する

US300cの初期設定では、ネットワーク設定は、「IPアドレスを自動的に取得する」に設定されています。ネットワーク設定を変更する場合は、以下の手順で変更してください。

1. US300cを接続するネットワークを確認して、LANケーブルをUS300cに接続する。
2. US300cの電源をONにする。
3. US300cのデスクトップが表示されたら、「スタート」→「コントロールパネル」→「ネットワーク接続」→「ローカルエリア接続」を実行し、「全般」タブの「プロパティ」ボタンをクリックする。

ネットワークに接続していない場合は、この操作は行うことができません。必ずネットワークに接続して操作を行ってください。

図1-7　ローカルエリア接続

4. 「ローカルエリア接続のプロパティ」ダイアログボックスが表示されるので、「Internet Protocol (TCP/IP)」を選択し、「プロパティ」ボタンをクリックする。

5. 「Internet Protocol(TCP/IP)のプロパティ」ダイアログボックスが表示されるので、ネットワーク環境に合わせて、IPアドレス、サブネットマスク、デフォルトゲートウェイ等の設定を行う。

仮想PC接続先を設定する

「スタート」メニューから「リモートデスクトップ接続」を起動して、接続する仮想PCの設定を行います。

1. 「スタート」メニューから「すべてのプログラム」をクリックし、「リモートデスクトップ接続」を起動する。

2. 「コンピューター(C)：」の欄に、接続する仮想PCのコンピューター名またはIPアドレスを入力する。

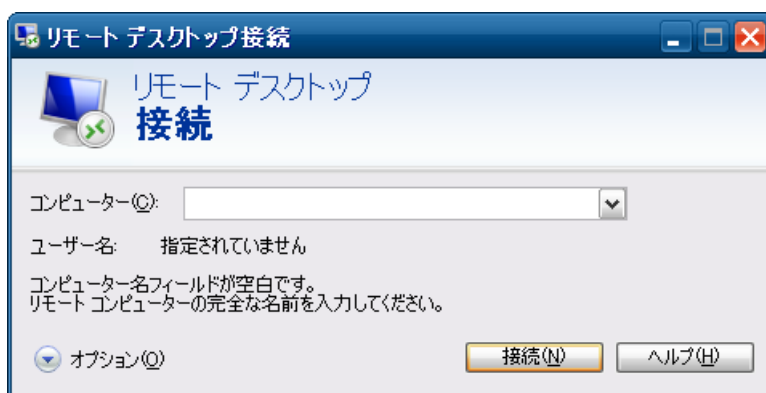



図1-8　リモートデスクトップ接続

- 仮想PC接続について詳細な設定を行う場合は、「オプション」ボタンをクリックして設定を行ってください。
- Citrixサーバーに接続する場合は、「スタート」メニュー→「すべてのプログラム」→「Online plug-in」を起動して接続先を設定してください。

仮想PCに接続する

前ページで設定した内容で、仮想PCに接続します。

1. 「リモートデスクトップ接続」を起動して、コンピューター名またはIPアドレスが表示されている状態で「接続」ボタンをクリックする。

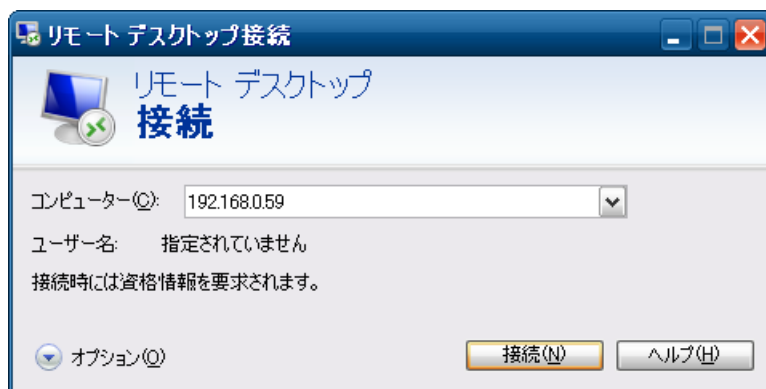



図1-9　リモートデスクトップ接続

仮想PCに接続され、仮想PCのログオンダイアログボックスが表示されます。

仮想PCにログオンした後は、仮想PCのデスクトップが表示され、「スタート」メニューから各種プログラムを使用することができます。

仮想PCをログオフする

仮想PCでの作業を終える場合は、仮想PCのデスクトップの「スタート」メニューから「ログオフ」を選択します。

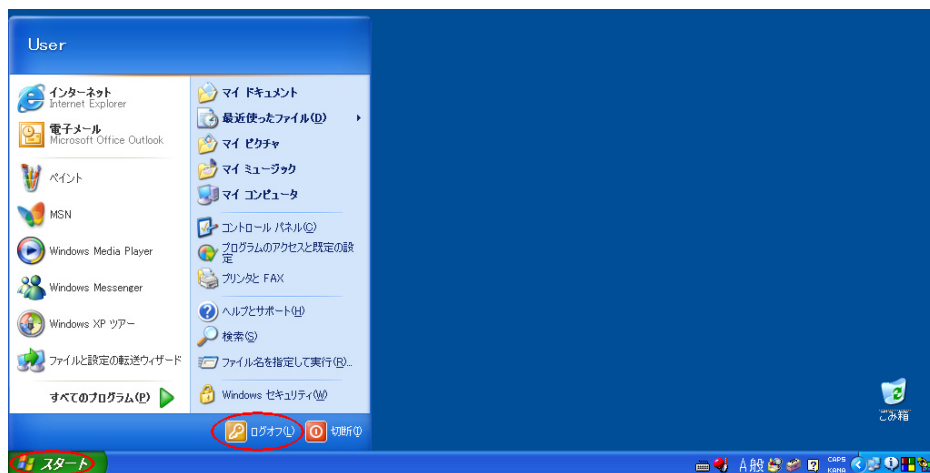



図1-10　仮想PCデスクトップ画面

仮想PCからログオフすると、US300cのデスクトップ画面に戻ります。

US300cをシャットダウンする

US300cの「スタート」メニューから「シャットダウン」を選択して、US300cをシャットダウンします。

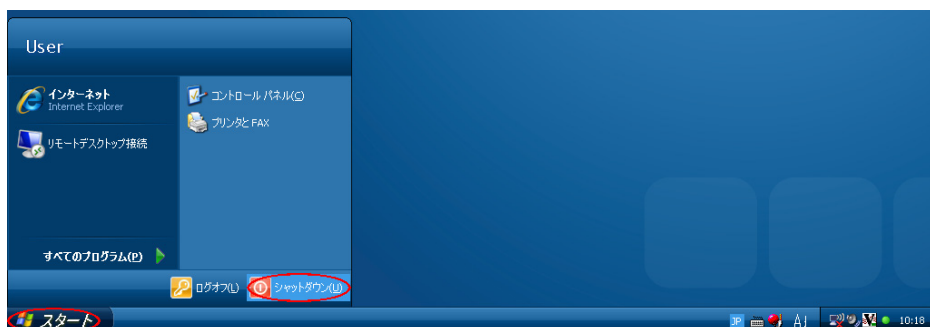



図1-11　US300c デスクトップ画面

2 サーバー環境の設定

サーバ環境の設定について説明しています。

企業サーバーへのアクセスの設定

US300cが使用できる企業サーバー環境への基本的なアクセス方法は、5つあります。イーサネット直接アクセス以外のアクセス方法では、すべてUS300c側で何らかのローカル設定を行う必要があります。このローカル設定は保持され、US300cシステムが次に起動するときに使用できます。ローカル設定および定義した接続は、US300cシステム起動時に自動で有効にすることもできます。

アクセス方法には、以下のものがあります。

イーサネット直接アクセス

US300cのイーサネットポートを使って企業イントラネットへ直接接続します。追加ハードウェアは必要ありません。この設定では、企業のDHCPサーバーを含むすべてのネットワークサービスを利用できます。ネットワーク上のDHCPサーバーは、US300cのIPアドレスだけではなく、ソフトウェアアップデートを格納するファイルサーバーの場所も提供できます。DHCPについては、「ダイナミックホストコンフィギュレーションプロトコル(DHCP)の使用方法」を参照してください。

ワイヤレス直接アクセス

ワイヤレスアダプタ(またはオプションの内蔵ワイヤレス機能)を使って企業イントラネットにアクセスします。
ワイヤレスネットワークデバイスの設定やオプションのUS300c内蔵ワイヤレス機能については、「ワイヤレスローカルエリアネットワーク(LAN)の設定」および「内蔵ワイヤレス機能の設定」を参照してください。

ワイヤレスアダプタは、短距離離広帯域無線を使用してワイヤレスアクセスポイントとの通信を行います。一般的に、ワイヤレスアクセスポイントは、企業内でワイヤレスアダプタの範囲内に複数あり、企業イントラネットに直接接続されます。

PPPoE

シンクライアントは、リモートからインターネットに直接接続するデバイス向けにPPPoEをサポートしています。いったん接続すると、すべてのパケットがPPP接続を通りイーサネットを経由してDSLモデムに送信されます。

接続方法

「新しい接続ウィザード」([スタート]→[コントロールパネル]→[ネットワーク接続]をダブルクリック→「ネットワークタスク」の[新しい接続を作成する]をクリック→[新しい接続ウィザード])を使って、PPPoE接続を設定して呼び出すことができます。
「新しい接続ウィザード」については、Microsoft社のWebサイトのマニュアルを参照してください(http://www.microsoft.com)。

ダイヤルアップモデム

ダイヤルアップモデムを使って、ダイヤルアップサーバーにアクセスできます。ダイヤルアップサーバーを使用して、以下のいずれかの接続方法で企業イントラネットにアクセスすることができます。

- 直接接続 ー 企業イントラネットに直接接続する企業ダイヤルアップサーバーを使用します。
- 間接接続 ー インターネットへの接続を提供するだけの、インターネットサービスプロバイダ(ISP)のダイヤルアップサーバーを使用します。US300cは、このサーバーを使って企業イントラネットに接続された企業のPPTP VPNサーバーにアクセスします。

ダイヤルアップサーバーは、Microsoft Remote Access Serverまたは業界標準プロトコルに対応したサーバーである必要があります。

PPTP VPN

PPTPは、US300cが必要とするネットワークサービスやセッションサービスを装備した企業サーバー環境への、企業ファイアウォールを通るパスワードで保護されたパスを提供します。

接続方法

「新しい接続ウィザード」([スタート]→[コントロールパネル]→[ネットワーク接続]をダブルクリック→「ネットワークタスク」の[新しい接続を作成する]をクリック→[新しい接続ウィザード])を使って、PPPoE接続を設定して呼び出すことができます。

- PPTP(Point-to-Point Tunneling Protocol)は、インターネットなどのTCP/IPベースのデータネットワークに広がる仮想プライベートネットワーク(VPN)を構築し、リモートクライアント(ここではUS300c)と企業サーバー環境間のセキュアなデータ転送を実現するネットワークプロトコルです。
- インターネットへアクセスするには、インターネットサービスプロバイダ(ISP)と契約する必要があります。ダイヤルアップモデム、ケーブルモデム、DSLモデムなどのISPへの標準的な接続方法はどれでも使用できます。企業のPPTP VPNサーバーにアクセスする前に、まずISPへの接続を確立する必要があります。この接続には、ダイヤルアップアクセスやケーブルモデムおよびDSLモデムパスによる直接アクセスなどがあります。「新しい接続ウィザード」については、Microsoft社のWebサイトのマニュアルを参照してください(http://www.microsoft.com)。

ネットワークサービスの設定方法について

US300cが使用するネットワークサービスには、DHCP、FTPファイルサービス、DNSなどがあります。ネットワークサービスの設定方法は、ご使用の環境で利用可能なものとそれをどのように設計・管理するかによって異なります。

以下の項目で、ネットワークサービスの設定に役立つ重要な情報を紹介します。

- 「ダイナミックホストコンフィギュレーションプロトコル(DHCP)の使用方法」
- 「FTPファイルサーバーの使用方法」
- 「ドメインネームシステム(DNS)の使用方法」

ダイナミックホストコンフィギュレーションプロトコル(DHCP)を使用する場合

初期状態のUS300c(新しいUS300cまたはデフォルト設定にリセットされたUS300c)はIPアドレスおよびネットワーク設定をDHCPサーバーから取得するように設定されています。また、以下の情報もDHCPサーバーから取得できます(Microsoft.msi形式)。

- FTPサーバーのIPアドレスやDNS名
- DHCPアップグレードプロセスによるアクセスに使用するアドオンのFTPルートパス

US300cの設定およびアップグレードには、DHCPを使用することをお勧めします。これにより、複数のUS300cでこれらの設定を行う手間を軽減できます。

DHCPサーバーを使用できない場合は、固定IPアドレスを割り当てることができます。固定IPアドレスは、デバイスごとにローカルに入力する必要があります。

Wyse Device Manager(WDM)サーバーのIPアドレスもDHCPサーバーから取得できます(WDMについては、「Wyse Device Managerソフトウェアを使用したリモート管理」を参照してください)。

US300cでは、表1のDHCPオプションを使用できます。

DHCPサーバーの設定については、Microsoft社のWebサイトのマニュアルを参照してください(http://www.microsoft.com)。

表1 DHCPオプション

オプション	説明	備考
1	サブネットマスク	必須項目です。
3	ルーター	設定は任意ですが推奨されるオプションです。US300cが別のサブネット上のサーバーと対話する必要がない限り、必要ありません。
6	DNSサーバー	設定は任意ですが推奨されるオプションです。
12	ホスト名	設定は任意です。
15	ドメイン名	設定は任意ですが推奨されるオプションです。
43	ベンダークラス固有の情報	設定は任意です。
50	要求されるIP	必須項目です。
51	リース時間	必須項目です。
52	オプションのオーバーロード	設定は任意です。
53	DHCPメッセージタイプ	必須項目です。
54	DHCPサーバーのIPアドレス	推奨オプションです。
55	パラメータ要求リスト	US300cによって送信されます。
57	最大DHCPメッセージサイズ	設定は任意です(常にUS300cによって送信されます)。
58	T1(更新)時間	必須項目です。
59	T2(リバインド)時間	必須項目です。
61	クライアント識別子	常に送信されます。
155	リモートサーバーのIPアドレスまたは名前	設定は任意です。
156	接続に使用するログオンユーザー名	設定は任意です。
157	接続に使用するドメイン名	設定は任意です。
158	接続に使用するログオンパスワード	設定は任意です。
159	接続用コマンドライン	設定は任意です。
160	接続用作業ディレクトリ	設定は任意です。
161	FTPサーバーリスト	設定は任意の文字列です。アップデートされたUS300cイメージが保存されるFTPサーバーの名前またはIPアドレスのいずれかです。名前を指定する場合は、オプション6で指定するDNSサーバーが解決できる名前を指定してください。
162	FTPファイルへのルートパス	設定は任意の文字列です。
163	SNMPトラップサーバーのIPアドレスリスト	設定は任意です。
164	SNMP設定コミュニティー	設定は任意です。
165	RDP起動公開アプリケーション	設定は任意です。
166	Ericom社PowerTerm® TECモード	設定は任意です。
167	Ericom社PowerTerm® TEC ID	設定は任意です。
168	仮想ポートのサーバー名	設定は任意です。

FTPファイルサーバーを使用する場合

Windows Embedded Standardには、Microsoft.msi形式のアドオンでUS300cをアップグレードするFTPアップグレードユーティリティが含まれています。このユーティリティで指定したFTPサーバーからMSIパッケージをダウンロードすることにより、US300cを自動または手動でアップグレードできます。MSIパッケージは、FTPサーバー上のFTPルートパス内のディレクトリに格納されます。

このFTPファイルサーバーの名前とルートパスディレクトリはUS300cで使用できるようにする必要があります。

必要なアップグレードオプションを選択するには、「FTP Addon Installer を使用したアドオンのインストールとアップグレード」の説明に従って、US300c上で[FTP Addon Installer]ダイアログボックスを使用して行います。

以下のガイドライン に従って、使用するサーバーを設定します。

- **自動アップグレード**

  US300cをアップグレードするには、Params.iniとMSIパッケージがFTPサーバー上(同じパス内)に存在する必要があります。

- **DHCPアップグレード**

  DHCPサーバーがMSIパッケージの場所を提供する場合は、表1　DHCPオプションに示す以下の設定をする必要があります(デフォルト)。

  161 - FTPサーバーリスト

  162 - FTPファイルへのルートパス

- **匿名ログオン機能**

  FTPサーバーには匿名ログオン機能が必要です。

- **ユーザーIDとパスワード**

  [FTP Addon Installer]ダイアログボックスのデフォルトのユーザー名は「anonymous」で、デフォルトのパスワードは「NEC」です。

DHCPを使用することをお勧めします。ただし、DHCPサーバーを使用できない場合は、US300c上で[FTP Addon Installer]ダイアログボックスを使って固定IPアドレス(FTPパス)を割り当てることができます。

ドメインネームシステム(DNS)を使用する場合

US300cは、企業イントラネットで利用可能なDNSサーバー上で登録されている有効なDNS名を受け付けます。US300cは、ネットワーク上のDNSサーバーに名前を照会してIPアドレスを解決します。ほとんどの場合、DNSは必須ではありませんが、DNSを使用すると、IPアドレスではなく登録したDNS名でホストにアクセスできます。

DNSドメインのDHCPエントリおよびサーバー場所情報については、「ダイナミックホストコンフィギュレーションプロトコル(DHCP)の使用方法」を参照してください。

Windows 2000以降のWindows DNSサーバーはすべてダイナミックDNS(DDNS)を装備しており、サーバーはすべてDNSサーバーに動的に登録されます。

セッションサービスについて

ICAおよびRDPセッションサービスを設定する前に、必ず以下のガイドラインを理解し、これに従ってください。

Windows Embedded Standardを実行するUS300cは、「VMware View Managerサービスの使用方法」に説明されているような仮想デスクトップソリューションもサポートしています。

● **全体的なガイドライン**

シンクライアントセッションサービスは、Citrix ICAおよびMicrosoft RDPソフトウェア製品のホストとして機能するサーバーによって提供されます。

● **ICAのガイドライン**

Independent Computing Architecture(ICA)は、アプリケーションのロジックをユーザーインタフェースから切り離す3層から成るサーバーベースのコンピューティング技術です。ユーザーは、US300cにインストールされているICAクライアントソフトウェアにより表示されるアプリケーションのGUIを操作できます。一方、すべてのアプリケーションプロセスはサーバー上で実行されます。ICAの設定については、「ICAセッションサービスの設定」を参照してください。

ICAサーバーのライセンスは、Citrix Systems, Inc.から取得する必要があります。Citrixサーバーファームに同時にかかるUS300cの負荷に対応できるだけのクライアントライセンスを購入してください。すべてのライセンスが使用中のときに接続が失敗するのは、US300cの故障によるものではありません。ICAクライアントソフトウェアは、US300cにインストールされます。

● **RDPのガイドライン**

Remote Desktop Protocol(RDP)は、US300cがWindows 2000/2003/Windows Server 2008 で動作するターミナルサービスとネットワーク経由で通信するためのネットワークプロトコルです。このプロトコルのベースとなるのは、国際標準のマルチチャネル会議プロトコルであるT.120プロトコルスイートです。US300cは、RDPバージョン7.xに対応しています。RDPの設定については、「RDPセッションサービスの設定」を参照してください。

ICAセッションサービスの設定

このセクションの情報を利用してICAセッションサービスを設定する前に、必ず「セッションサービスについて」をお読みください。

ICAセッションサービスは、ターミナルサービスと以下のいずれかがインストールされている状態で、Windows Server 2003 または Windows Server 2008を使用してネットワーク上で利用できます。

- **Citrix XenApp 5.0**

  製品に付随する指示に従って上記の製品をインストールし、サーバー環境を共有するUS300cにセッションおよびアプリケーションを提供します。

Windows Server 2003 または Windows Server 2008を使用する場合や、Citrix XenApp 5.0をWindows Server 2008と使用する場合は、ネットワーク上のアクセス可能な場所にターミナルサービスクライアントアクセスライセンス(TSCAL)サーバーが常駐している必要があります。このサーバーは、デバイス単位で一時ライセンス(120日間有効)を付与します。この一時ライセンスの有効期間(120日間)が終了した後は、TSCALを購入してTSCALサーバーにインストールする必要があります(一時ライセンスまたは永久ライセンスなしで接続することはできません)。

サーバー環境の設定

RDPセッションサービスの設定

このセクションの情報を利用してRDPセッションサービスを設定する前に、必ず「セッションサービスについて」をお読みください。

RDPセッションサービスは、以下の端末にリモート接続するときに使用されます。
（Windows XP Professional、Windows Vista、およびWindows 7）
Remote Desktop Protocolにより、US300cはWindowsアプリケーションをWindows GUI環境下で実行できます。ただし、実際にはこれらのWindowsアプリケーションは接続しているコンピュータ上で実行されています。

製品に付随する指示に従って上記の製品をインストールし、サーバー環境を共有するUS300cにセッションおよびアプリケーションを提供します。

VMware® View Managerサービスの使用方法

VMware® View Managerは、システム管理者がデスクトップを設定し、ユーザーアクセスを制御するためのデスクトップ管理ソリューションです。クライアントソフトウェアは、中央の仮想デスクトップ、バックエンドの物理システム、またはターミナルサーバーにユーザーをセキュアに接続します。

View Managerのインストールおよび設定については、VMwareのWebサイトを参照してください（http://www.vmware.com）。

View Managerは、以下の主要なコンポーネントで構成されています。

- **View Connection Server**

  クライアント接続のブローカとして機能するソフトウェアサービスで、入って来たリモートデスクトップユーザー要求を認証し、仮想デスクトップ、物理デスクトップ、またはターミナルサーバーに適宜振り分けます。

- **View Agent**

  ゲスト仮想マシン、物理システム、または ターミナルサーバーにインストールされるソフトウェアサービスで、それらすべてをView Managerで管理できるようにします。RDP接続の監視、仮想印刷、リモートUSBのサポート、シングルサインオンなどの機能を提供します。

- **View Client**

  View Connection Serverと通信する、ローカルでインストールするソフトウェアアプリケーションで、ユーザーがMicrosoftリモートデスクトッププロトコル（RDP）を使用してデスクトップに接続できるようにします。

- **View Client with Offline Desktop**

  ユーザーが仮想マシンをダウンロードしてローカルシステムで使用するためのオフラインデスクトップ機能をサポートするために拡張されたView Clientの1つのバージョンです。

- **View Portal**

  複数のオペレーティングシステムおよびブラウザによってサポートされているView ClientのWeb版です。

- **View Administrator**

  View Managerの管理者がView Connection Serverを設定し、デスクトップを展開および管理し、ユーザー認証を制御し、システムイベントを開始および検査し、分析処理を行うためのWebアプリケーションです。

- **View Composer**

  VirtualCenterサーバーにインストールされるソフトウェアサービスで、View Managerが、リンクされている複数のクローンデスクトップを中央の1つのベースイメージから迅速に展開できるようにします。

3 導入

使用する際の基本的な設定を説明しています。

電源投入時の処理

US300cを起動した時やリブート時に最初に表示される内容は、企業イントラネットへのアクセス方法や、ネットワーク管理者がユーザーアカウントをどのように設定しているかによって異なります。

- WDMソフトウェアを使用している場合は、Wake-On-LAN機能を使用してリモートでUS300cの電源を入れることもできます。
- WDMに未登録の場合、ネットワークに接続した状態で起動するとOSの起動に長時間(2分程度)かかることがあります。

ログオン

管理者は、「ユーザーマネージャによるユーザーとグループの管理」の説明に従ってユーザーアカウントを作成した後、「Winlogによる自動ログオンの有効／無効化」の説明に従って、ユーザーアカウントに対し自動ログオンか、ユーザー認証情報(ユーザー名、パスワード、ドメイン)に基づく手動ログオンかを設定できます。

US300cのデフォルトでは､ユーザーデスクトップへの自動ログオンが有効になっています。管理者としてログオンするには､SHIFTキーを押しながらユーザーデスクトップをログオフして[Windowsへログオン]ダイアログボックスを表示し､管理者認証情報を入力してログオンします(デフォルトのユーザー名とパスワードはどちらも「Administrator」です 。)。

セキュリティ上、各US300cで管理者のパスワードをデフォルトから変更することをお勧めします(新たに設定した管理者パスワードを忘れると管理者としてログオンすることができなくなるので、ご注意ください)。管理者としてＵＳ３００ｃにログオンし、CTRL+ALT+DELキー→[Windows のセキュリティ]ウィンドウ→[パスワードの変更]→[パスワードの変更]ダイアログボックスでパスワードを変更します。「US300cの設定」で説明しているように、US300cでパスワードを変更する前に必ずFile Based Write Filter(FBWF)を無効にし、パスワード変更後に再度有効にしてください。

自動ログオン

US300cのデフォルトでは、ユーザーデスクトップへの自動ログオンに設定されています。[自動ログオン]が有効な状態で別のユーザーとしてログオンするには、SHIFTキーを押しながら現在のデスクトップをログオフし、[Windowsへログオン]ダイアログボックスを表示し、認証情報を入力してログオンします。

管理者は、ログオンしてWinlogを使用し(管理者用コントロールパネルにあります)、自動ログオンを有効または無効にし、US300cに自動ログオンするユーザー名、パスワード、およびドメインを変更できます。US300cの自動ログオンのプロパティを変更できるのは、管理者のみです。

US300cで行った設定(自動ログオンのプロパティなど)をUS300cのリブート後も維持するには、「US300cの設定」で説明しているように、必ずUS300cの設定変更の前にFBWFを無効にし、設定変更後に再度有効にしてください。

手動ログオン

自動ログオンが有効でない場合は、US300cの起動時に[Windowsへログオン]ダイアログボックスが表示されます。

以下のガイドラインに従ってください。

- ユーザーアカウントの場合、デフォルトのユーザー名とパスワードはどちらも「User」です 。
- 管理者アカウントの場合、デフォルトのユーザー名とパスワードはどちらも「Administrator」です 。

パスワードでは大文字小文字が区別されます。ユーザー名では大文字小文字は区別されません。

US300cの設定

ユーザーでログオンして行った設定は、ログオフして同じまたは別のユーザーとして再度ログオンする操作では失われませんが、リブート後は維持されません。管理者でログオンしている場合、リブート後も維持される設定が可能です。

以下のガイドラインに従ってください。

1. 管理者としてログオンします。US300cに最初にログオンする場合や、管理者権限を持たないユーザーでUS300cにログオンしている場合は、SHIFTキーを押しながらユーザーデスクトップをログオフし、[Windowsへログオン]ダイアログボックスを表示し、管理者認証情報を入力してログオンする必要があります(デフォルトのユーザー名とパスワードはどちらも「Administrator」です 。)。

US300cのデフォルトでは、ユーザーデスクトップへの自動ログオンが有効になっています。管理者は、Winlogを使用し(管理者用コントロールパネルにあります)、自動ログオンを有効または無効にし、US300cに自動ログオンするユーザー名、パスワード、およびドメインを変更できます。たとえば、管理者はWinlogを使用し、起動時に[Windowsへログオン]ダイアログボックスを表示して管理者認証情報を使用してログオンできるようにUS300cを設定できます。

2. US300cにログオン後、デスクトップの[FBWF を無効]アイコンをダブルクリックしてFBWFを無効にします(これによりフィルタが無効になり、システムがリブートされます)。

3. US300cでユーザーデスクトップへの自動ログオンが有効な場合は、ユーザーデスクトップをログオフし、管理者としてログオンする必要があります(SHIFTキーを押しながらユーザーデスクトップをログオフして[Windowsへログオン]ダイアログボックスを表示し、管理者認証情報を使用してログオンします)。

4. 本書の指示に従って、US300cを設定します。たとえば、「アドオンのインストールとアップグレード」を参照し、アドオンを自動的にアップグレードするようUS300cを設定することができます。

5. 設定完了後、デスクトップの[FBWF を有効]アイコンをダブルクリックしてFBWFを有効にします(これによりフィルタが有効になり、システムがリブートされます)。US300c上の設定が保存され、US300cのリブート後も維持されます。

FBWFについては、「File Based Write Filter(FBWF)の使用方法」を参照してください。

ユーティリティの自動起動について

以下のユーティリティは自動的に起動されます。

- **FBWF**

  FBWFユーティリティは、システム起動時に自動的に起動されます。このユーティリティは、フラッシュメモリへの誤った書き込みからUS300cを保護することにより、US300cでのコンピュータ処理にセキュアな環境を提供します。フィルタの有効／無効状態は、タスクバーのシステムトレイ内にある[File Based Writer Filter Control]アイコンの色によって示されます。FBWFについては、「File Based Write Filter（FBWF）の使用方法」を参照してください。

カレントシステムセッションでFBWFキャッシュのファイルを一括書き込み（フラッシュ）してコミットしなければ、US300c設定の変更は、US300cの再起動時に失われます。一括書き込みの手順については、「US300cの設定」および「File Based Write Filter（FBWF）の使用方法」を参照してください。

- **NetXClean**

  NetXCleanユーティリティは、システム起動時に自動的に起動されます。NetXCleanは、ローカルディスクに関係ない情報を格納しないようにするクリーンアップユーティリティです。特定のプロファイル設定（プリンタなど）を維持したい場合は、必ず明示的に宣言したプロファイルを消去しないようにNetXCleanを設定してください。NetXCleanについては、「NetXCleanユーティリティについて」を参照してください。

- **VNC Server**

  Windows VNC Server ユーティリティは、US300cに正常にログオンすると、自動的に起動されます。VNCは、管理およびサポート目的でUS300cデスクトップにリモートアクセスできるようにするユーティリティです。VNCについては、「WinVNCを使用したUS300cのリモートシャドー」を参照してください。

- **時間同期ユーティリティ**

  必要に応じて、管理者は時間同期ユーティリティの機能をローカルまたはリモートで無効にできます。時間同期については、「NeutronとのUS300c時間の同期」を参照してください。

ユーザーデスクトップについて

デフォルトのユーザーデスクトップには、[Online plug-in]や[リモートデスクトップ接続](標準およびFor Dual Monitor)などのアイコンがあります。[スタート]メニューには、Internet Explorer、コントロールパネル、[プリンタとFAX]などの項目があります。[すべてのプログラム]メニューには、Online plug-in、このデバイスについて、Internet Explorer、リモートデスクトップ接続(標準およびFor Dual Monitor)、アクセサリ、スタートアップ、Windows Media Playerなどのメニューがあります(Ericom社のPowerTerm® Terminal EmulationやVMwareアプリケーションがインストールされている場合は、[すべてのプログラム]からアクセスできます)。タスクバーのシステムトレイには、音量、TightVNCサービス、FBWFの状態、およびシステム時刻が表示されます。

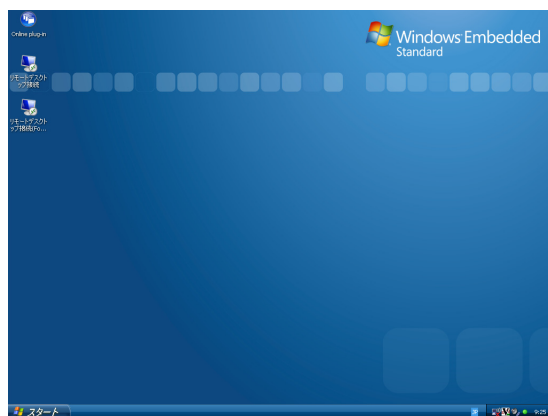



図3-1　ユーザーデスクトップの例

ICA公開アプリケーションへのリンクも、[スタート]メニューやデスクトップアイコンに表示される場合があります。

以下のガイドラインに従ってください。

- ユーザー用コントロールパネル([スタート]→[コントロールパネル])から、ユーザー選択設定を行うための限定的なリソースセットにアクセスできます。
- ユーザーデスクトップを右クリックしても、コンテキストメニューは開きません。
- リモートセッションとローカルマシン間では、Windowsの標準コピー&ペースト機能を使用してテキストのコピー、貼り付けができます。

標準的なWindows Embedded Standardデスクトップの機能および[スタート]メニュー項目については、Microsoft社のマニュアルを参照してください(http://support.microsoft.comのマイクロソフトサポートオンライン)。

Online plug-inについては、「Online plug-in接続を使用した管理」を参照してください。

リモートデスクトップ接続については、「リモートデスクトップ接続の確立」を参照してください。

管理者デスクトップについて

デフォルトの管理者デスクトップには、[Online plug-in]、[リモートデスクトップ接続](標準およびFor Dual Monitor)、[FBWF を無効]、[FBWF を有効]などのアイコンがあります。[スタート]メニューには、Internet Explorer、[マイ コンピュータ]、[マイ ネットワーク]、コントロールパネル、[プリンタとFAX]、[検索]、[ファイル名を指定して実行]などのメニューがあります。[すべてのプログラム]メニューには、Online plug-in、このデバイスについて、Internet Explorer、リモートデスクトップ接続(標準およびFor Dual Monitor)、アクセサリ、スタートアップ、Windows Media Player、[WinVNC Current User Properties]などのメニューがあります(Ericom社のPowerTerm® Terminal EmulationやVMwareアプリケーションがインストールされている場合は、[すべてのプログラム]メニューからアクセスできます)。タスクバーのシステムトレイには、音量、TightVNCサービス、FBWFの状態、およびシステム時刻が表示されます。

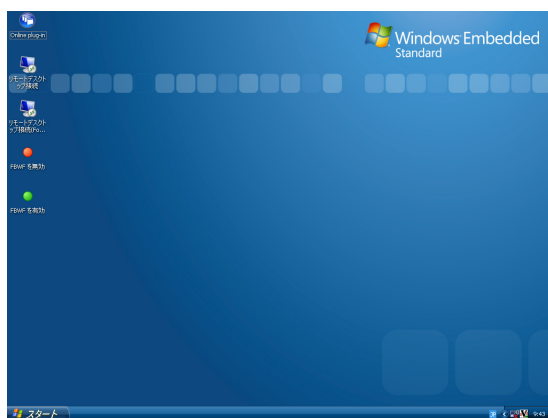



図3-2　管理者デスクトップの例

以下のガイドラインに従ってください。

- 管理者用コントロールパネル([スタート]→[コントロール パネル])から、ユーザー選択設定およびシステム管理を設定するための広範なリソースセットにアクセスできます。
- 管理者デスクトップを右クリックすると、コンテキストメニューが開きます。
- リモートセッションとローカルマシン間では、Windowsの標準コピー&ペースト機能を使用してテキストのコピー、貼り付けができます。

標準的なWindows Embedded Standardデスクトップの機能および[スタート]メニュー項目については、Microsoft社のマニュアルを参照してください(http://support.microsoft.comのマイクロソフトサポートオンライン)。

Online plug-inについては、「Online plug-in 接続を使用した管理」を参照してください。

リモートデスクトップ接続については、「リモートデスクトップ接続の確立」を参照してください。

ログオフ、シャットダウン、および再起動

[シャットダウン]メニューを使用すると、US300cをログオフ、シャットダウン、再起動、およびスタンバイ状態にすることができます(いずれも[スタート]→[シャットダウン]をクリック)。[Windowsのセキュリティ]ウィンドウ(CTRL+ALT+DELキー)からUS300cをログオフまたはシャットダウンすることもできます。

自動ログオンが有効な場合は、(シャットダウンせずに)ログオフすると、US300cが即座にデフォルトのユーザーデスクトップにログオンします。別のユーザーとしてログオンする手順については、「ログオン」を参照してください。

休止状態も選択できますが、選択しないでください。休止状態はサポートしていません。

以下のユーティリティは、US300cのログオフ、再起動、シャットダウン時に影響を受けます。

- **FBWFキャッシュ**

  システム設定を変更し、リブート後もその変更を維持するには、カレントシステムセッション中にFBWFキャッシュのファイルを一括書き込みする必要があります。ファイルを一括書き込みしないと、変更した設定はUS300cのシャットダウンまたは再起動時に失われます。FBWFキャッシュの内容は、単にログオフして同じまたは別のユーザーとして再度ログオンしただけでは失われません。したがって、再度ログオンした後でFBWFキャッシュのファイルを一括書き込みしても変更を維持できます。一括書き込みの手順については、「FBWFのコントロールの設定」を参照してください。FBWFについては、「File Based Write Filter(FBWF)の使用方法」を参照してください。

ユーザーは、FBWFキャッシュのファイルを一括書き込みできません。この操作は、管理者機能です。

- **NetXCleanユーティリティ**

  NetXCleanは、フラッシュメモリに関係ない情報を格納しないようにするクリーンアップユーティリティです。クリーンアップは、再起動、シャットダウン、またはユーザーによるログオフ時に自動的に実行されます。特定のプロファイル設定(プリンタなど)を維持したい場合は、必ず明示的に宣言したプロファイルを消去しないようにNetXCleanを設定してください。NetXCleanについては、「NetXCleanユーティリティについて」を参照してください。

- **電源管理**

  電源管理は、モニター への映像信号を切り、指定したアイドル時間の経過後にモニターを節電モードにすることができます。設定は、[スタート]→[コントロール パネル]→[画面]→[スクリーン セーバー]→モニタ電源の[電源]→[モニタの電源を切る]で行うことができます。

● Wake-on-LAN

この標準的なWindows Embedded Standard機能により、Wyse Device Managerソフトウェアは、シャットダウンされた、またはスタンバイ状態のデバイスでイメージアップデートおよびリモート管理機能を実行できます。この機能を使用するには、US300cに電源供給がされている必要があります。

Wake-on-LANでWakeさせた後はWindowsを起動させてください。BIOS Set upやDOSを起動しただけの場合はDC-offできません。

● US300c の日付時刻

シャットダウンした後も、電源に接続されたままの状態である限り、クロック時間は維持されます。電源がオフで、かつ電力供給がない場合は、クロック時間が失われます。ローカル時間ユーティリティを設定すると、指定時間に自動的に、または手動でタイムサーバーにUS300c の日付時刻を同期させることができます。

US300c の日付時刻を参照する必要があるアプリケーションもあるので、正確な時刻を維持するようにしてください。[日付と時刻のプロパティ]ダイアログボックスは、タスクバーのシステムトレイの[時刻]が表示されている箇所をダブルクリックするか、コントロール パネルの[日付と時刻]アイコンをダブルクリックすると開くことができます。

4 各種機能の利用

各種機能の利用について説明しています。

すべてのプログラム

US300cの「すべてのプログラム」から、次のプログラムが起動できます。

- Internet Explorer
- Online plug-in
- このデバイスについて
- リモートデスクトップ接続
- リモートデスクトップ接続（For Dual Monitor）
- Accessories
- Ericom - PowerTerm® Terminal Emulation
- Ericom PowerTerm® WebConnect Client
- VMware
- スタートアップ
- Microsoft Baseline Security Analyzer 2.1
- Neutron
- Windows Media Player

コントロールパネル

US300cのコントロールパネルから、次のプログラムが起動できます。

- Diagnostic Tool
- Windows CardSpace
- インターネットオプション
- キーボード
- ゲームコントローラ
- スキャナとカメラ
- データソース（ODBC）
- ネットワーク接続
- プリンタとFAX
- マウス
- ユーザー補助のオプション
- ワイヤレスリンク
- 音声認識
- 画面
- 地域と言語のオプション
- 日付と時刻
- 電源オプション
- サウンドとオーディオデバイス

以降のページで各プログラムの詳細について説明します。

Internet Explorer

Internet Explorer を起動して、インターネットのWebサイト等に接続することができます。

図4-1　Internet Explorer

インターネットに接続するにはネットワークが適切に設定されている必要があります。

Online Plug-in (Citrixサーバーへの接続)

Citrix Online Plug-inを使用して、Citrix Xen Appに接続できます。

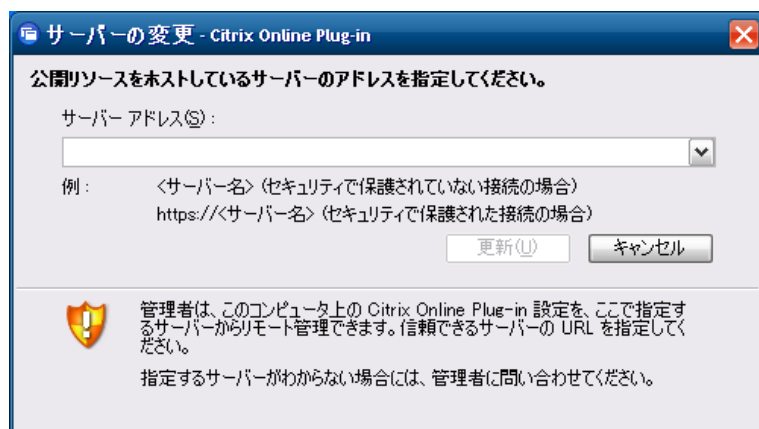



図4-2　Citrix Online Plug-in

CtrixサーバーにPNAgentのサイトが作成されている必要があります。

このデバイスについて

US300cのWDMを使用してのアップデート、FTP Addon Insteller でインストールしたアプリケーションのシステム情報およびバージョン情報を参照できます(「スタート」→「すべてのプログラム」→「このデバイスについて」)。

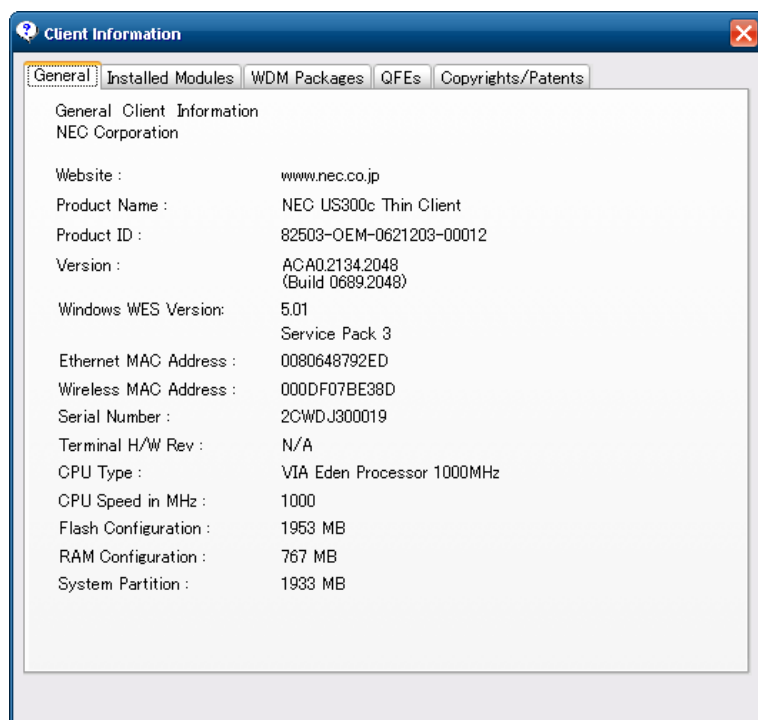



図4-3　このデバイスについて

リモートデスクトップ接続

仮想PCへ接続するために使用します。
「リモートデスクトップ接続」の「オプション」を選択すると、以下の画面が現れます。

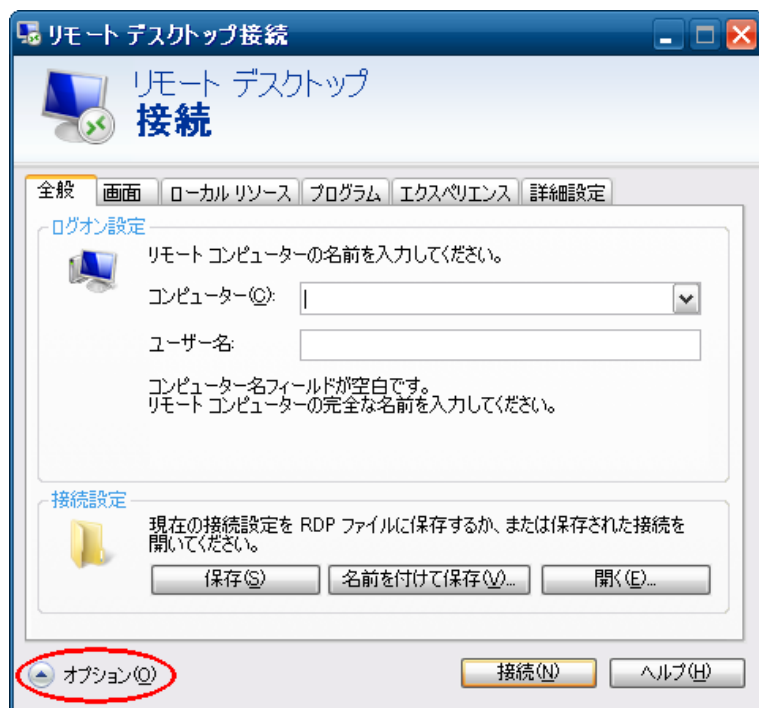



図4-4　リモートデスクトップ接続

リモートデスクトップ接続 (For Dual Monitor)

デュアルディスプレイを使用して、仮想PCへ接続する時に使用します。
「リモートデスクトップ接続」の「オプション」を選択すると、以下の画面が現れます。

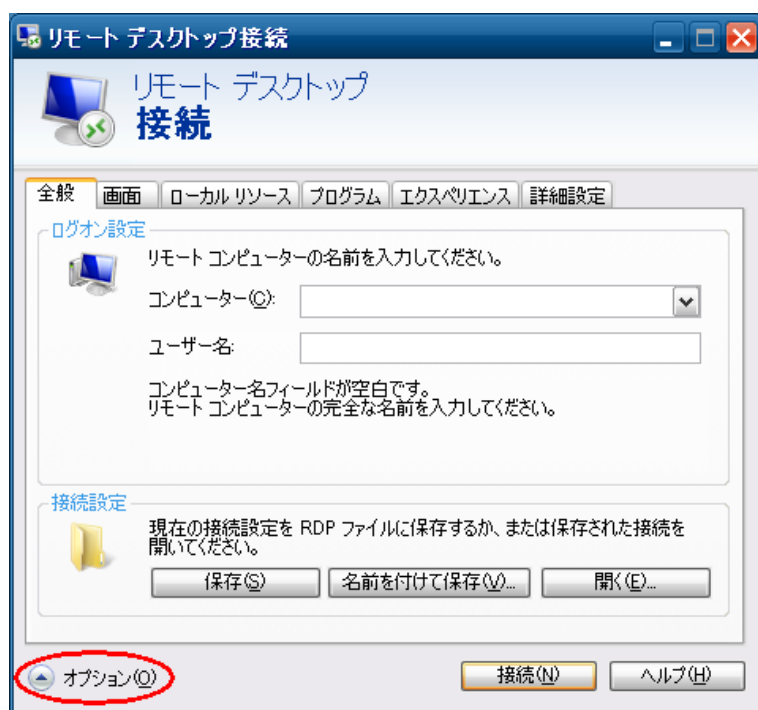



図4-5　リモートデスクトップ接続 (For Dual Monitor)

デュアルディスプレイを使用した仮想PCへの接続方法については、「第5章　仮想PC接続でのデュアルディスプレイの利用」(102 ページ) を参照してください。

Accessories

Accessories内にある次のプログラムを起動することができます。

- Internet Explorer （アドオンなし）

Ericom ─ PowerTerm® Terminal Emulation

PowerTerm Session ManagerおよびPowerTerm Emulationを使用できます。

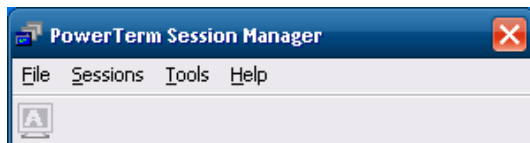



図4-6　PowerTerm Session Manager

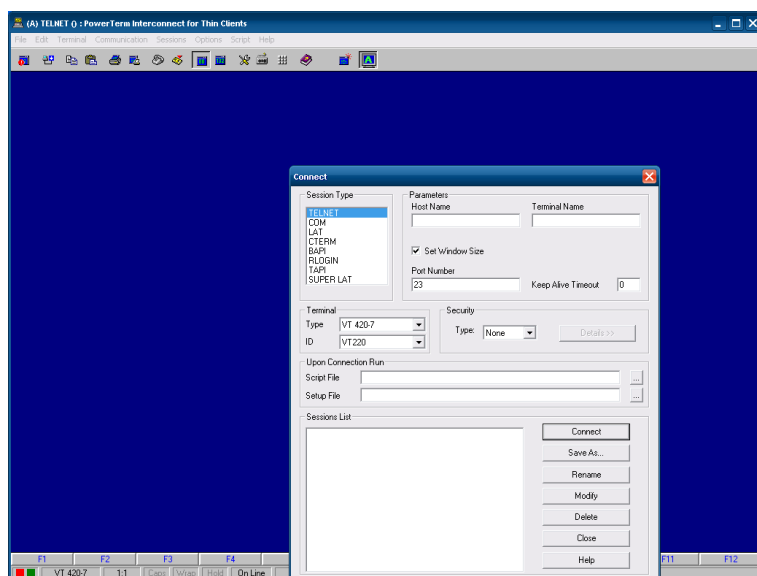



図4-7　PowerTerm Emulation

PowerTerm Session ManagerおよびPowerTerm Emulationの設定、および使用方法については Ericom社のWebサイトを参照してください。
（http://www.ericom.com/）

Ericom PowerTerm® WebConnect Client

PtStartを使用できます。

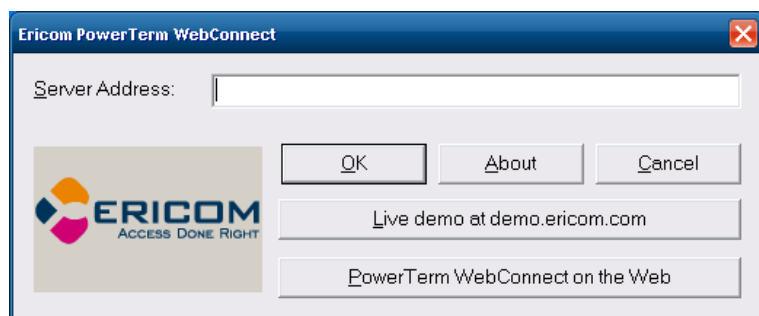



図4-8　PtStart

PtStartの設定、および使用方法については Ericom社のWebサイトを参照してください。
（http://www.ericom.com/）

各種機能の利用

VMware

VMware View Clientを使用できます。

図4-9　VMware View Client

VMware View Clientの設定、および使用方法については、VMwareのWebサイトを参照してください。
（http://www.vmware.com）

スタートアップ

ログオン時に自動起動するプログラムを設定します。初期状態ではスタートアップに設定されているプログラムはありません。
Administratorユーザーがスタートアップを設定できます。

Microsoft Baseline Security Analyzer 2.1

Microsoft Baseline Security Analyzer 2.1 が使用できます。

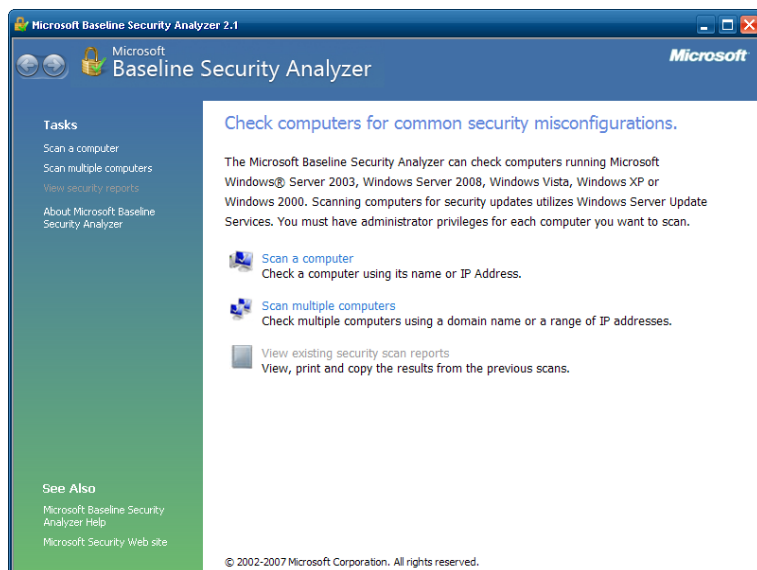



図4-10　Microsoft Baseline Security Analyzer 2.1

Microsoft Baseline Security Analyzer 2.1の設定、及び使用方法については、Microsoft社のWebサイトを参照してください。
（http://microsoft.com/）

Neutron

Neutronを使用して、US300c の時刻同期を行うことができます。

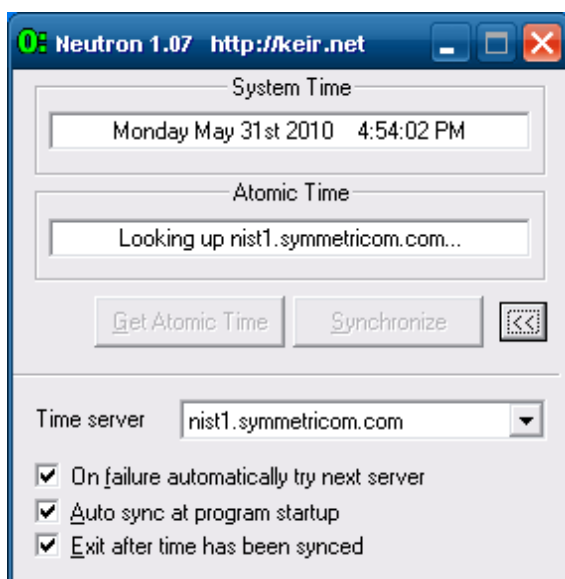



図4-11　Neutron

Neutron の設定、及び使用方法については「6 WESの拡張機能の紹介 Neutronによる US300cの日付時刻の同期」(124ページ)の箇所を参照してください。

Windows Media Player

Windows Media Player を使用することができます。

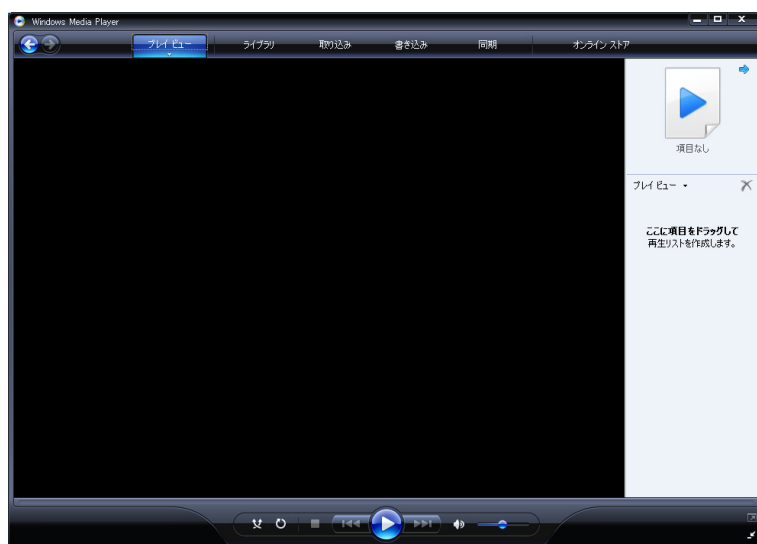



図4-12　Windows Media Player

Diagnostic Tool

Diagnostic Tool を使用できます。

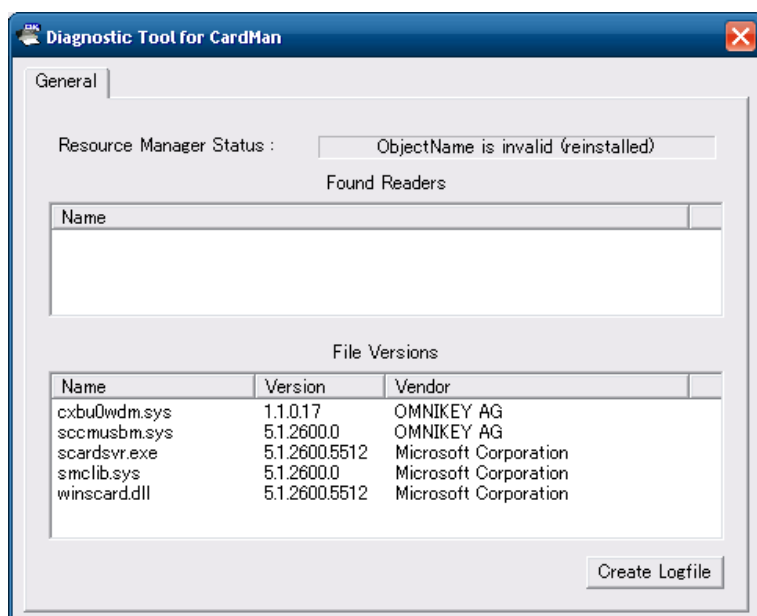



図4-13　Diagnostic Tool

Diagnostic Toolの設定、および使用方法等については、OMNIKEY社のWebサイトを参照してください。
（http://www.hidglobal.com/omnikey）

各種機能の利用

Windows CardSpace

Windows CardSpace が使用できます。

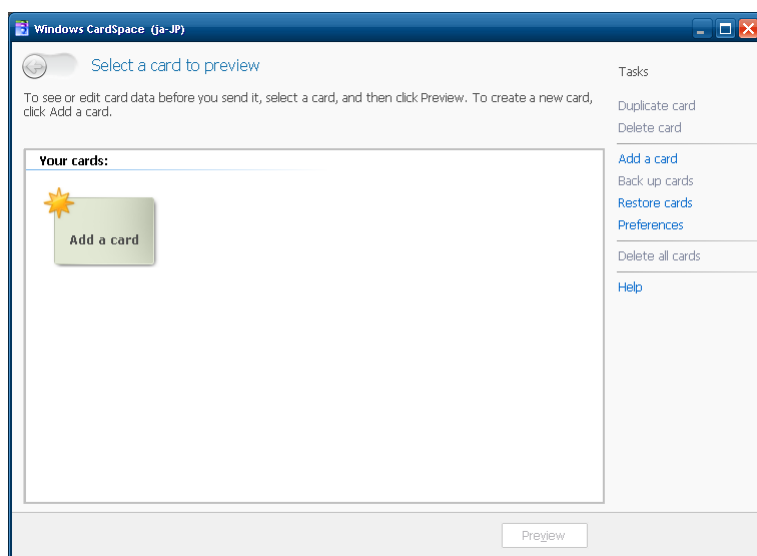



図4-14　Windows CardSpace

Windows CardSpaceの設定、および使用方法等については、Microsoft社のWebサイトを参照してください。
（http://microsoft.com/）

インターネットオプション

インターネットエクスプローラのオプションが設定できます。

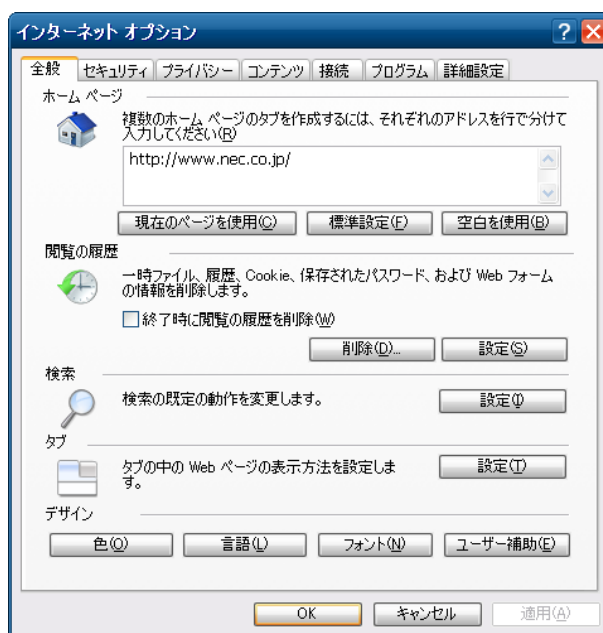



図4-15　インターネットオプション

キーボード

キーボードのキーリピート等について設定できます。

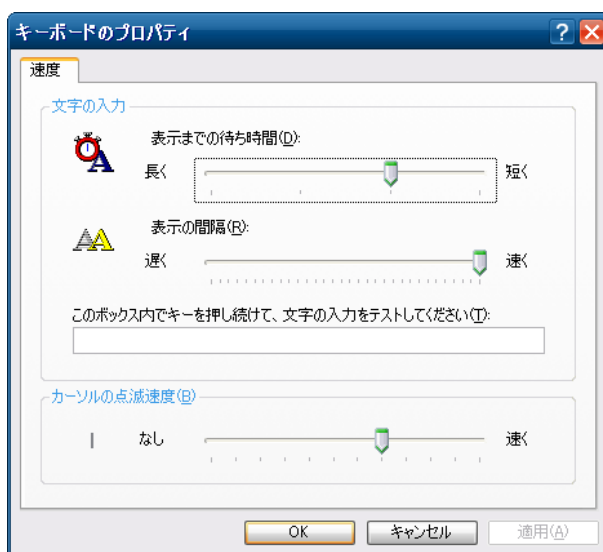



図4-16　キーボード

ゲームコントローラ

ゲームコントローラの追加や削除、プロパティの設定などを行うことができます。

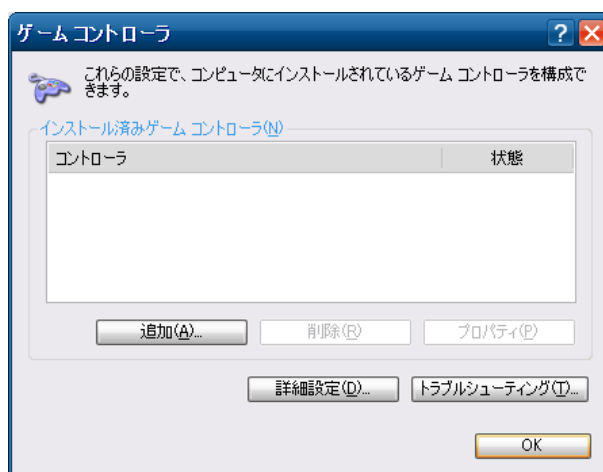



図4-17　ゲームコントローラ

スキャナとカメラ

スキャナやカメラの追加や削除、プロパティの設定などを行うことができます。

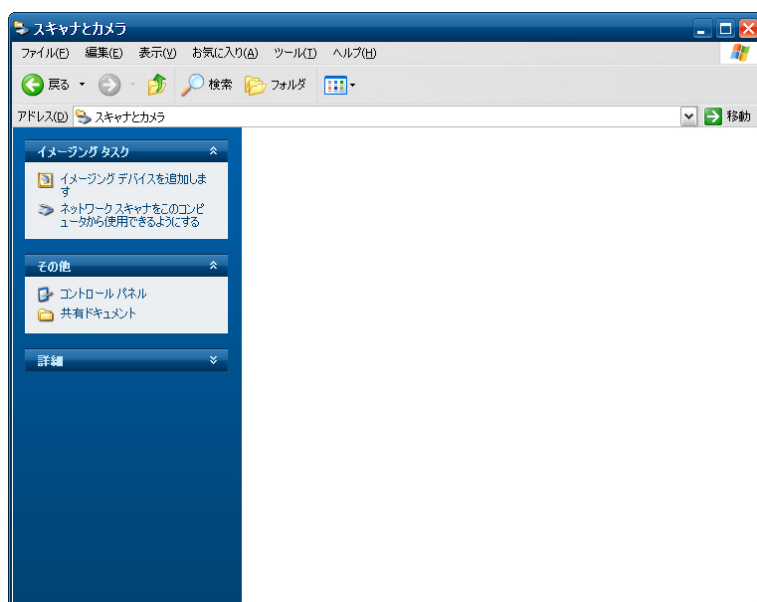



図4-18　スキャナとカメラ

データソース(ODBC)

データソース(ODBC)に関する設定を行うことができます。

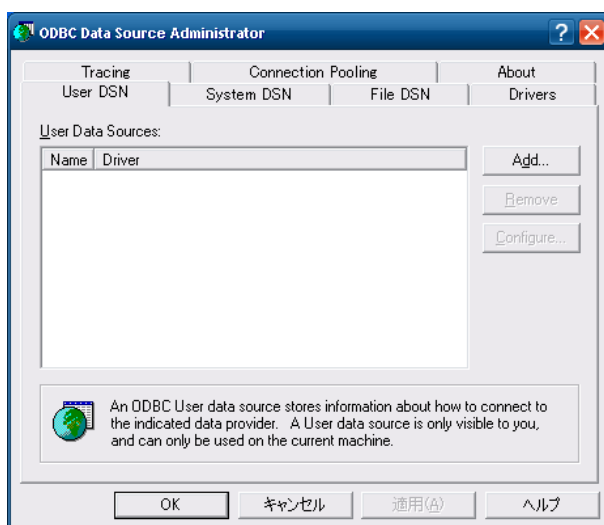



図4-19　データソース(ODBC)

データソース(ODBC)の設定、および使用方法等については、Microsoft社のWebサイトを参照してください。(http://microsoft.com/)

ネットワーク接続

ネットワーク接続の設定をすることができます。

図4-20　ネットワーク接続

「ワイヤレスネットワーク接続」は、無線LANが内蔵されているUS300cのみ表示されます。

ローカルエリア接続

US300cの有線LANの設定を行います。IPアドレス、DNSサーバー等が設定できます。
設定方法は、「第1章 ネットワークを設定する」(35ページ)を参照してください。

図4-21　ローカルエリア接続

ワイヤレスネットワーク接続

US300cで無線LANを使用する場合は、ここで使用するネットワークを設定します。
接続するワイヤレスネットワークの選択、接続の詳細設定、IPアドレス等が設定できます。

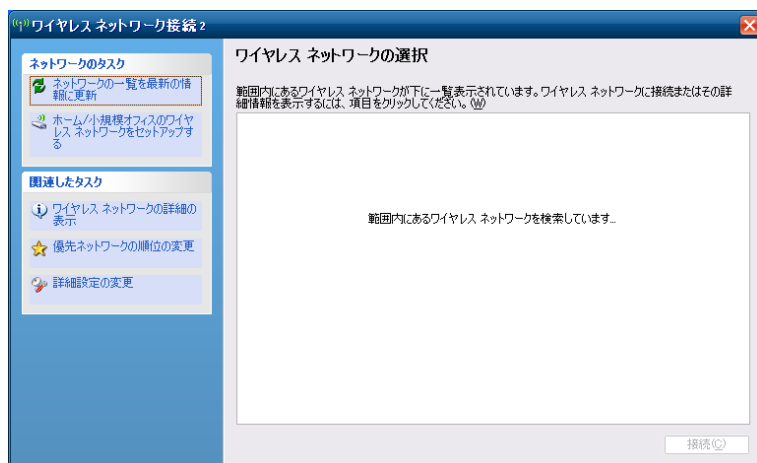



図4-22　ワイヤレスネットワーク接続

ワイヤレスネットワーク接続の設定方法

以下の手順で設定してください。

1. 範囲内にあるワイヤレスネットワークの一覧から、接続するネットワークを選択し、[接続]をクリックする。
   接続するネットワークが表示されていない場合は、「ネットワークのタスク」より「ネットワークの一覧を最新の情報に更新」を選択し、ネットワークの一覧を更新してください。

2. ネットワーク管理者によって無線LANに接続するためのネットワークキーが設定されている場合、ネットワークキーの入力ダイアログが表示されるので、ネットワークキーを入力する。

3. ワイヤレスネットワーク接続画面にて「接続」と表示されたことを確認する。
   ワイヤレスネットワーク接続画面に「接続」と表示されたら、ワイヤレスネットワークへの接続は完了です。

- 接続するネットワークにより、設定の方法が異なる場合があります。設定の方法が異なる場合はネットワークの管理者に確認してください。
- [ワイヤレス ネットワーク セットアップ]ウィザードは使用できません。
- 「6 WES の拡張機能の紹介 内蔵ワイヤレス機能の設定」(139ページ)も合わせて参照ください。

プリンタとFAX

プリンタとFAXの追加や削除、プロパティの設定などを行うことができます。

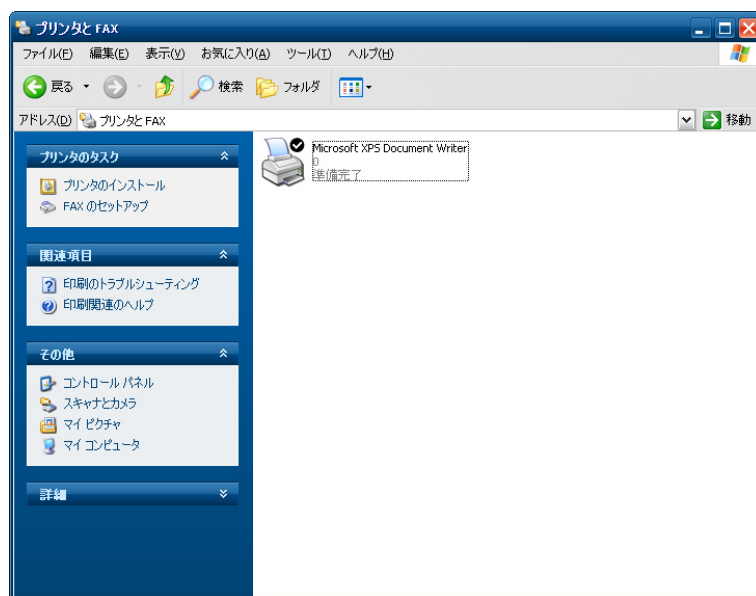



図4-23　プリンタとFAX

ここでは、US300cで新しいプリンタやその他のデバイスを追加する方法を説明します。

1. 「Administrator」でログオンする

2. US300cのライトフィルタを無効に設定する。(デスクトップ画面　→　「FBWFを無効」アイコンをダブルクリック。)

3. 使用するデバイスをUS300cに接続する。

4. 「新しいハードウェアの検出ウィザード」が起動しますので、ウィザードに従って、ドライバのインストールを行う。

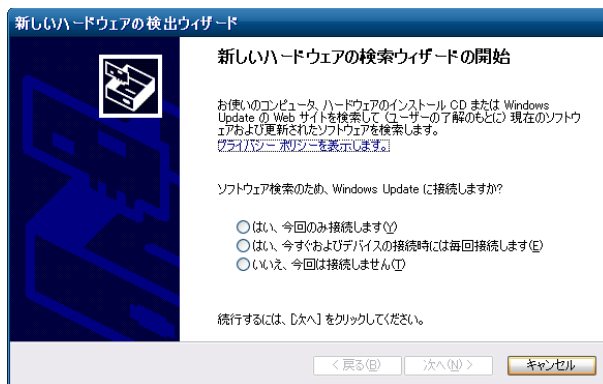



図4-24　新しいハードウェアの検出ウィザード

5. ドライバのインストール後、US300cのライトフィルタを有効にする。(デスクトップ画面　→「FBWFを有効」アイコンをダブルクリック。

デバイスドライバをインストールする場合は、ライトフィルタを無効にした状態でインストールを行ってください。

マウス

マウスのダブルクリックの速さ、ポインタオプション等が設定できます。

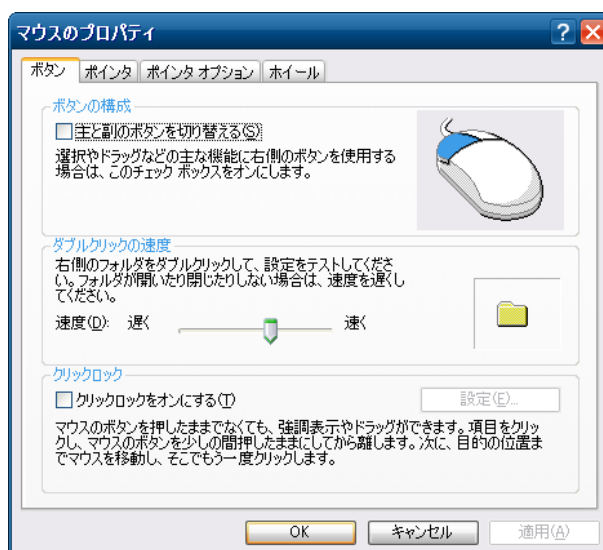



図4-25　マウス

ユーザー補助のオプション

ユーザー補助のオプションの設定ができます。

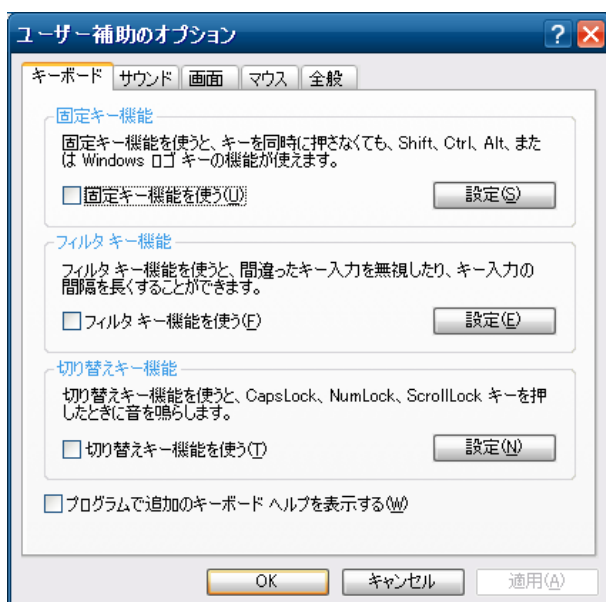



図4-26　ユーザー補助のオプション

ワイヤレスリンク

ワイヤレスリンクの設定ができます。

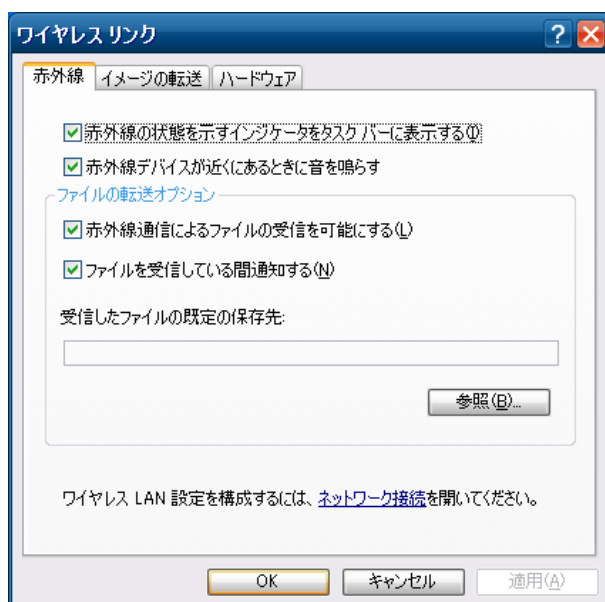



図4-27　ワイヤレスリンク

赤外線ポートはUS300cに標準内蔵されていないため、オプション品なしにワイヤレスリンクの機能は使用できません。

音声認識

音声認識の設定ができます。

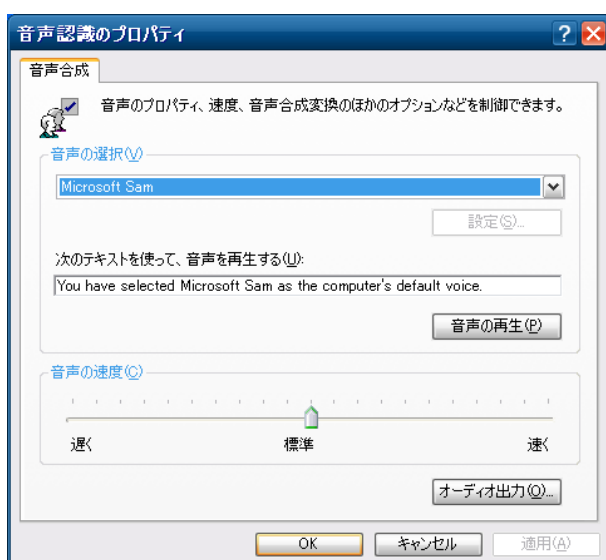



図4-28　音声認識

画面に関する設定(画面の背景、スクリーンセーバー、画面の解像度など)ができます。

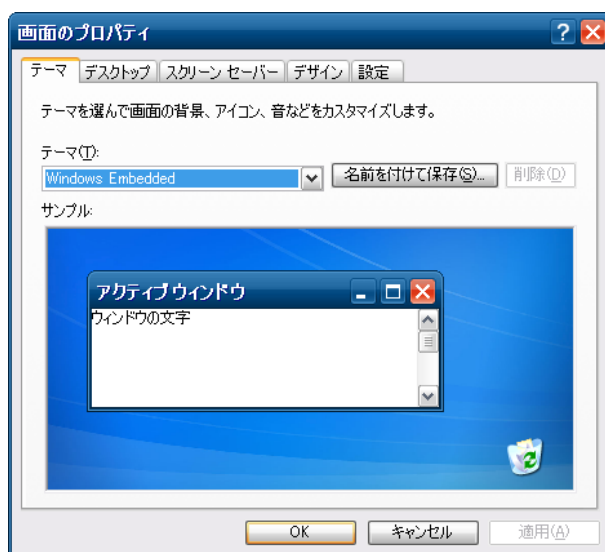



図4-29　画面

電源オプション

省電力の設定ができます(「スタート」→「コントロールパネル」→「画面」→「スクリーンセーバー」タブ→モニタ電源の「電源」ボタン)。

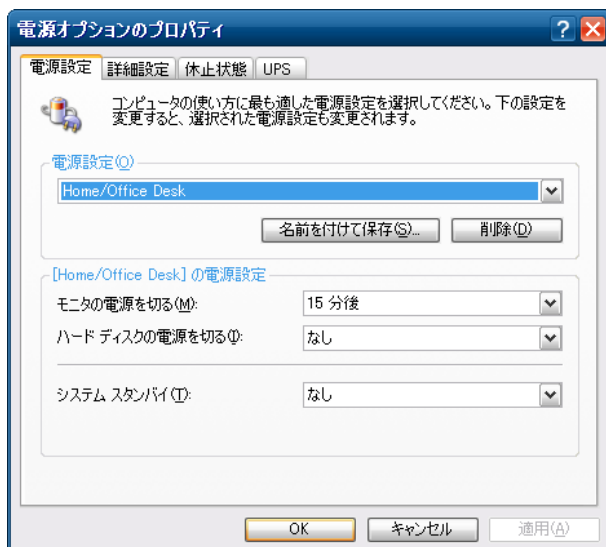
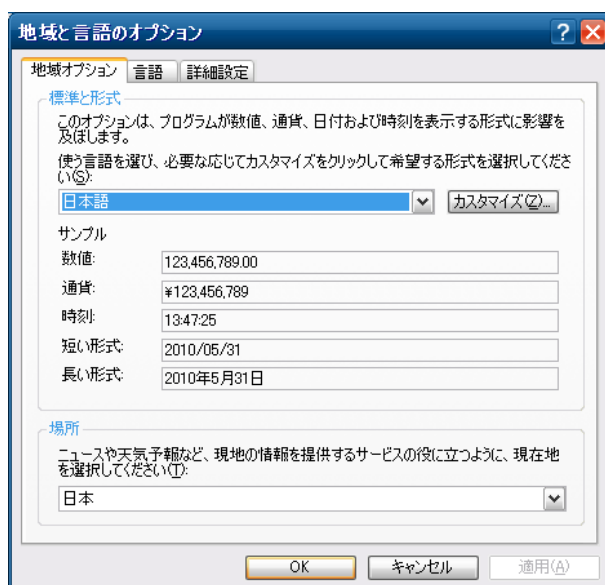



図4-30　電源オプション

地域と言語のオプション

地域と言語のオプションの設定ができます。

図4-31　地域と言語のオプション

各種機能の利用

日付と時刻のプロパティ

US300cの日付時刻、タイムゾーン、タイムサーバーの使用について設定できます。

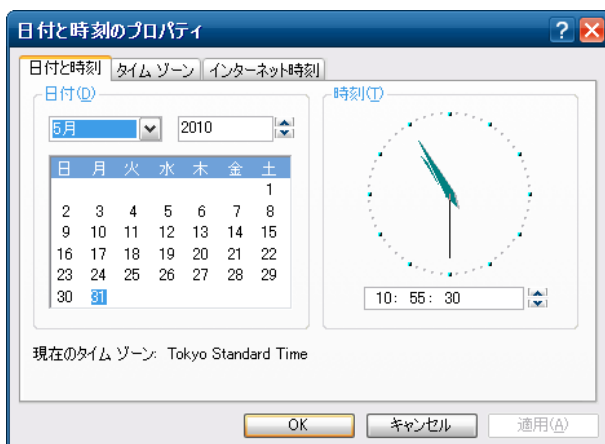



図4-32　日付と時刻

サウンドとオーディオデバイス

US300cの音量等のサウンド、オーディオについて設定できます。
サウンドとオーディオデバイスは次の方法で起動することができます。

1. タスクバーのスピーカーアイコンを右クリック　→　「オーディオプロパティの調整」
2. 「スタート」メニュー　→　「コントロールパネル」をカテゴリ表示　→　「サウンド、音声、および オーディオデバイス」　→　「サウンドの設定を変更する」

図4-33　サウンドとオーディオデバイス

5 応用機能の利用

応用機能の利用について説明しています。

仮想PC接続でのデュアルディスプレイの利用

US300cの仮想PC接続において、デュアルディスプレイを使用する方法を参考情報として記載します。

US300cでは、リモートデスクトップによる仮想PC接続でデュアルディスプレイを使用することができます。

重要

- **プライマリディスプレイとセカンダリディスプレイの解像度の設定が異なる場合、リモートデスクトップのデュアルディスプレイ表示はできません。**
- **プライマリディスプレイとセカンダリディスプレイの配置の設定が画面のプロパティの設定どおりに左右に並んでいない場合、デュアルディスプレイ表示はできません。**
- **VGAとDVI-Iのアナログ出力でのデュアルディスプレイには対応しておりません。VGAとDVI-Iのデジタル出力でご利用ください。**

仮想PC接続をデュアルディスプレイモードで使用する場合は、以下の手順で仮想PCに接続します。

1. US300cにセカンダリディスプレイを接続する。
2. [スタート]→[コントロールパネル]→[画面]を選択し、画面のプロパティを起動する。
3. [設定]タブで、セカンダリディスプレイを選択し、「Windowsデスクトップをこのモニタ上で移動できるようにする」を選択する。
4. セカンダリディスプレイの解像度をプライマリディスプレイと同じ解像度に設定する。
5. プライマリディスプレイとセカンダリディスプレイを「画面のプロパティ」の配置通りに並べる。

図5-1　画面のプロパティ

6. 「OK」ボタンをクリックし、画面のプロパティを終了させる。

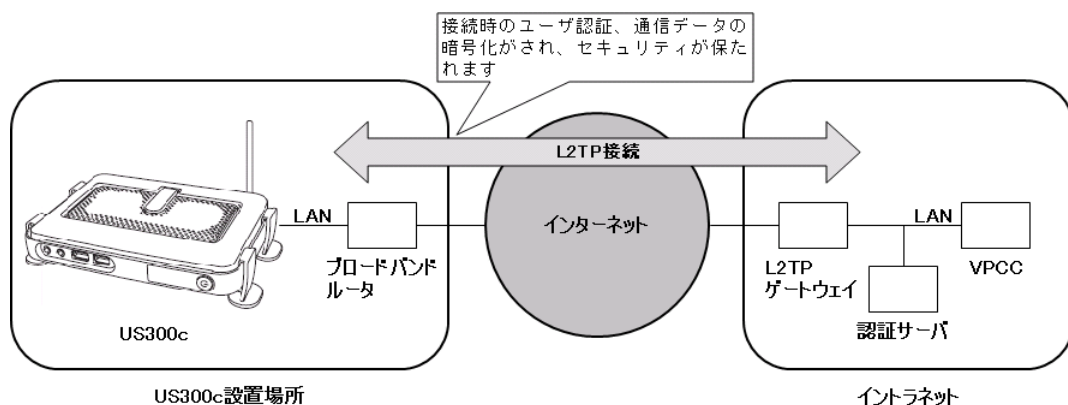
7. [スタート]→[すべてのプログラム]→[リモートデスクトップ接続(For Dual Monitor)]を起動する。

8. 「リモートデスクトップ接続」ダイアログが表示されるので、コンピュータ名等、必要な情報を入力し、仮想PCへ接続する。

VPN接続

ここでは、VPN接続について説明します。

VPN接続のシステム構成図

US300cをインターネット経由で会社内のVPCCに接続する場合のネットワーク構成として、「L2TP+IPSec方式」を用いた方式を示します。

L2TP+IPSec方式でUS300cがVPN接続を行うと、イントラネットのIPアドレスが付与されて、イントラネットに接続している状態と同じになり、VPCCとアクセスすることができます。

構成

US300c設置場所：

- ブロードバンドルータ： インターネットとの接続を行います。

イントラネット：

- L2TPゲートウェイ
  - インターネットとの接続を行います。認証サーバーと連携して、US300cとのVPN通信を行います。
  - データ暗号化にはIPSecを使用します。IPSec認証方式としては、「Preshared Key(事前鍵共有方式)」を使用します。ここで設定したPreshared Keyの文字列は、US300cにも設定します。
  - US300cへのIPアドレスの払い出し方針を選択します(L2TPゲートウェイで設定する方式と、外部認証サーバーで設定する方式から選択をします)。
  - ユーザ認証方式にはRADIUSを利用します。RADIUSの認証プロトコルは「PAP」を使用します。
  - ユーザ認証を外部のRADIUSサーバーを利用する場合には、L2TPゲートウェイで接続設定を行います。
- RADIUS認証サーバー
  - インターネット接続時のユーザ認証を行います。 L2TPゲートウェイからの認証要求に応答するように設定します。

設定は、それぞれの装置の設定方法に従ってください。

US300cのVPN設定方法

ここでは、VPNの設定方法について説明します。

VPN(L2TP)接続の作成

以下の手順でVPN(L2TP)接続を作成します。

1. US300cのライトフィルタを無効化する。(ライトフィルタの設定は「デスクトップアイコンによるFBWFの有効/無効化」(153ページ)を参照して下さい。)
2. Administratorでログオンする。
3. 「スタート」メニュー → 「コントロールパネル」 → 「ネットワーク接続」を選択する。
4. 「ネットワーク接続」画面が表示されるので、「ファイル」メニューから「新しい接続」を選択する。
新しい接続ウィザードが起動します。
5. 新しい接続ウィザードの開始画面で「次へ(N)」ボタンをクリックする。

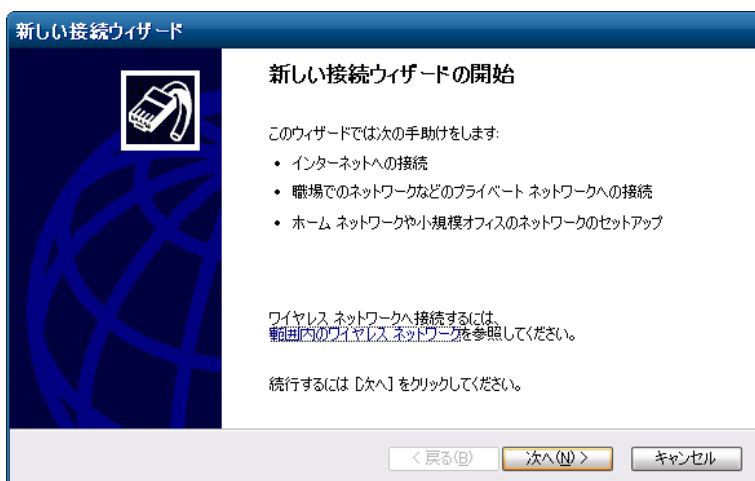



図5-2　新しい接続ウィザードの開始

6. ネットワーク接続の種類の選択画面で「職場のネットワークへ接続する(O)」を選択し、「次へ(N)」ボタンをクリックする。

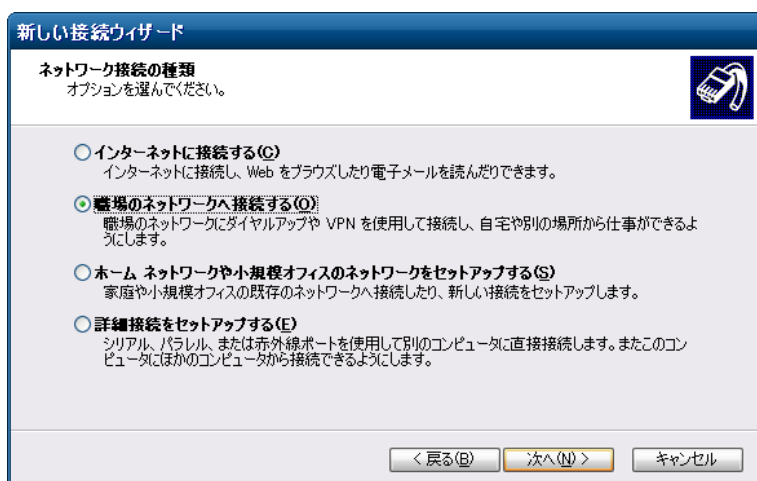



図5-3　ネットワーク接続の種類

7. ネットワーク接続の選択画面で「仮想プライベートネットワーク接続(V)」を選択し、「次へ(N)」ボタンをクリックする。

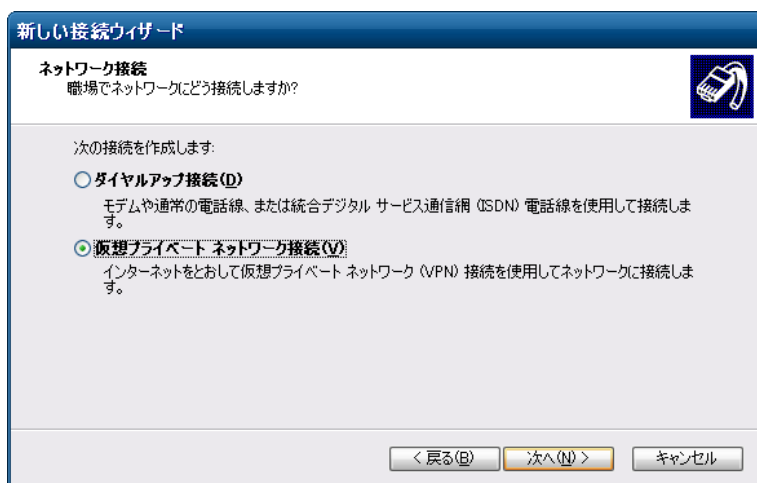



図5-4　ネットワーク接続

8. 接続名入力画面にて接続の名前を入力し、「次へ(N)」ボタンをクリックする。

図5-5　接続名

9. VPNサーバーの選択画面で、VPNサーバーの名前またはIPアドレスを入力し、「次へ(N)」ボタンをクリックする。

図5-6　VPNサーバーの選択

10. 新しい接続ウィザードの完了画面で「完了」ボタンをクリックする。

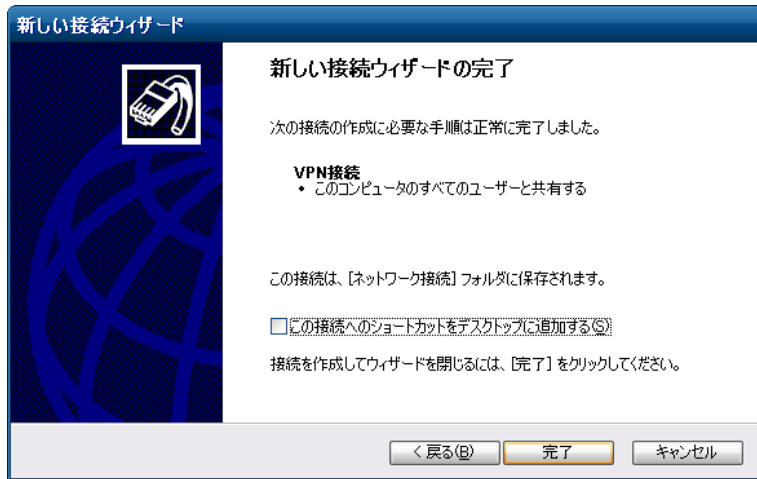



図5-7　新しい接続ウィザードの完了

11. [接続]ウィンドウで、「プロパティ(O)」ボタンをクリックする。

図5-8　接続ウィンドウ

12. [(接続名)プロパティ]ウィンドウで[セキュリティ]タブを選択し、「IPSec設定(P)」ボタンをクリックする。

13. [IPSec設定]ウィンドウで「認証に事前共有キーを使う」を選択して、L2TPゲートウェイに設定したPreshared Keyの値を入力して「OK」ボタンをクリックする。

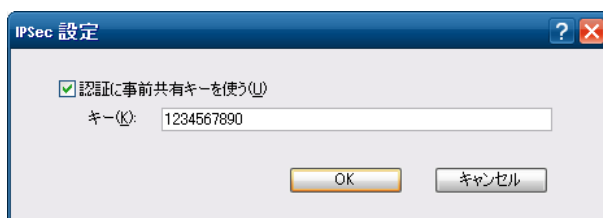



図5-9　IPSec設定ウィンドウ

14. [(接続名)プロパティ]ウィンドウの[ネットワーク]タブを選択し、[VPNの種類(E)]から「L2TPIPSec VPN」を選択し、「OK」ボタンをクリックする。

図5-10　VPNの種類

15. US300cのライトフィルタを有効化する。(ライトフィルタの設定は「デスクトップアイコンによるFBWFの有効／無効化」(153ページ)を参照して下さい。)

US300cのVPN接続方法

以下の手順でVPN接続を行います。

1. 「ネットワーク接続」画面を開き、先ほど作成した接続アイコンをクリックする。
   作成したＶＰＮ接続を「スタート」メニューに追加されている場合は、「スタート」メニューの「すべてのプログラム」より追加された接続を選択してください。

2. 管理者から通知されたL2TP接続用のユーザ名、パスワードを入力し、「接続(C)」ボタンをクリックする。

図5-11　仮想プライベートネットワークへの接続

VPN接続の設定を変更する場合は、接続の作成時と同様にライトフィルタを無効化してから設定を変更してください。設定変更後、ライトフィルタを有効化してください。

RDP暗号化レベルの設定

Windows Server 2003のターミナルサービスを利用している場合には、ターミナルサービス構成にて暗号化レベルの設定ができます。

[ターミナルサービス構成]→[接続]→[RDP-Tcpプロパティ]→[全般タブ]に暗号化レベルがあります。
「FIPS準拠/高/クライアント互換/低」の4つの選択値が存在し、デフォルトはクライアント互換です。

Windows XPでは、グループポリシーにて暗号化レベルの設定ができます。

mmcを起動し、「ファイル」メニューの「スナップインの追加と削除」で、グループポリシーオブジェクトエディタを追加します。

[ローカルコンピュータポリシー]→[コンピュータの構成]→[管理用テンプレート]→[Windowsコンポーネント]→[ターミナルサービス]→[暗号化とセキュリティ]に「クライアント接続の暗号化レベルを設定する」があります。

この設定を有効にし、暗号化レベルを「クライアント互換/高レベル/低レベル」から、選択してください。

時刻同期

インターネット時刻サーバーに接続して時刻の同期をとる場合は、以下の手順を行ってください。

1. [スタート]→[コントロールパネル]→[日付と時刻]を選択し、「日付と時刻のプロパティ」を起動する。

2. [インターネット時刻]タブを選択して下記項目を設定し、「OK」ボタンをクリックする。
   これにより、インターネット時刻サーバーに接続して時刻の同期をとるように設定することができます。

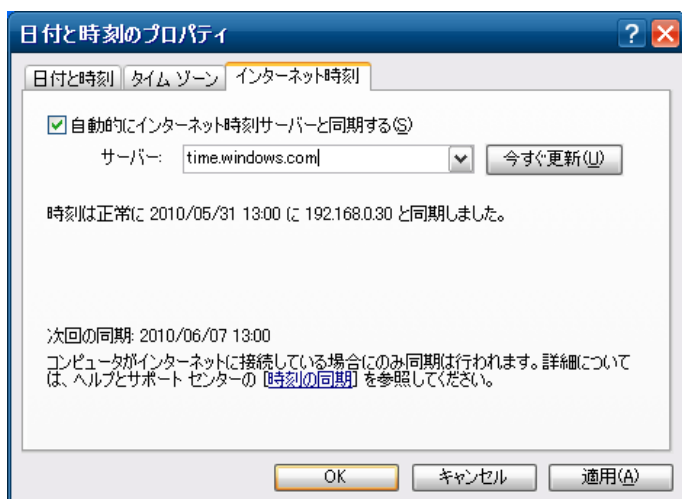



図5-12　インターネット時刻

- **「自動的にインターネット時刻サーバーと同期する」チェックボックス**

  このチェックボックスにチェックを入れることによって、自動的にタイムサーバー(インターネット時刻サーバー)と同期をとることができます。

- **「サーバー:」**

  時刻同期を行うインターネット時刻サーバー名を入力します。

- **「今すぐ更新」ボタン**

  直ちにインターネット時刻サーバーへアクセスし、時刻を設定します。

現在の日付とUS300cのシステムの日付に大きな差異がある時に、インターネット時刻サーバーとの時刻同期に失敗する事があります。失敗が発生する場合は、システムの日付を手動で現在の日付に合わせて頂いた後インターネット時刻サーバーとの時刻同期を行ってください。

ソフトウェアアップデート

US300cは、ソフトウェアをアップデート、追加インストールするために、WDM、または FTP Addonsを使用することができます。

- WDMを使用しての配信方法などの詳細はシンクライアントシステムのサポート情報ページ(http://www.nec.co.jp/products/thinclient/support/)を参照ください。
- FTP Addonsは管理者ユーザーのみ使用可能なツールです。

WDMを使用したアップデート

以下の手順でWDMを使用したアップデート配信を行います。

1. WDM にアップデートモジュールを登録する。
2. 登録を行ったアップデートモジュールをアップデートする US300c に対して配信設定を行い配信を実行する。

FTP Addonsを使用したアップデート

以下に示す設定を行ってください。

US300c「FTP Addons」の設定

1. 管理者としてログオンし、[スタート]メニュー → [コントロールパネル] → [FTP Addons] を起動します。

2. アップデートの設定を確認してください。
アップデートを行う環境に合わせて、各内容を設定してください。

● [Manual FTP Information]

DHCPオプションを使用しない場合は、こちらを選択し、各項目を設定してください。

● [Use DHCP Server's FTP Options]

DHCPオプションを使用する場合は、こちらを選択してください。

[FTP Path]テキストボックスは無効となり、DHCPサーバーから取得されるFTPサーバー名およびパスが表示されます

(DHCPオプション161(FTPサーバーリスト)および162(FTPファイルへのルートパス)を設定する必要があります)。

● [FTP Path：]

FTPファイルへのルートパスを、IPアドレスから入力してください。

[Use DHCP Server's FTP Options]が選択されている場合はグレーアウトされ、DHCPサーバーから取得されるFTPサーバー名およびパスが表示されます

● [User name：]

FTPサーバーにアクセスするユーザー名を入力します。

デフォルトでは「anonymous」が入力されています。

● [Password]

FTPサーバーにアクセスするユーザーのパスワードを入力します。

デフォルトでは「NEC」が入力されています。

● [Save Password]

認証情報を入力せずにFTPサーバーにログオンできるように設定する場合はチェックします。

● [Settings]

接続再試行回数と再試行の間隔を設定することができます。

インストールするアプリケーションによっては、インストールに失敗する可能性があります。その場合は、「7章」の「追加ソフトウェアの利用」を参照してインストールを行ってください。

応用機能の利用

ソフトウェアアップデートの実行

手動アップデート

1. 管理者としてログオンし、[スタート]メニュー → [コントロールパネル] → [FTP Addons] を起動します。

2. 「Upgrade」ボタンを押下します。
US300cがリブートされ、Write Filterが無効になります。リブート処理には約5秒かかります。
アップデート後、US300cがリブートされ、Write Filterが有効になります。

自動アップデート

1. 管理者としてログオンし、[スタート]メニュー → [コントロールパネル] → [FTP Addons] を起動します。

2. [Allow Automatic Upgrade] をチェックします。

3. 「Add」ボタンを押下します。

4. [Add-on-upgrade FTP info] ダイアログ内の各項目を設定します。

   設定する内容は 2.1 US300c「FTP Addons」の設定 を参照してください。

5. [Auto add-on upgrade list] に情報が追加されることを確認します。

6. [OK]をクリックし、US300cを再起動します。

7. US300c起動時に [Auto add-on upgrade list] 内のすべてのソフトウェアに対し、最新バージョンの有無を自動的にチェックします。リスト内のソフトウェアがインストールされていない場合や、インストール済みのソフトウェアの最新バージョンがFTPサーバーに存在する場合は、自動アップデートが実行されます。
自動アップデートが実行されると、US300cがリブートされ、Write Filterが無効になります。
リブート処理には約5秒かかります。アップデート後、US300cがリブートされ、Write Filterが有効になります。

- FTPサーバー上のMSIパッケージには同じパス上にあるParams.iniファイルを付ける必要があります。Params.iniファイルがないと、インストールは失敗します。
- 「8 システム管理 アドオンの自動インストールとアップグレード」(173ページ)の項目にも関連する情報が記載されています。

6 WESの拡張機能の紹介

WESの拡張機能について説明しています。

周辺機器の設定と使用方法

US300cは、USBポートを経由してサービスを提供できます。

各種サービスのアドオンをインストールすることができます(アドオンはWyse社 から提供されており、無償のものと有償のものがあります)。使用可能なアドオンについては、Wyse社のWebサイト(http://www.wyse.com/products/software/firmware/) を参照してください。

[すべてのプログラム]メニューの拡張機能の利用

このセクションでは、[すべてのプログラム]メニュー内の拡張機能([スタート]→[すべてのプログラム]から使用できるオプション)の概要を紹介します。

- 「Online plug-inを使用した接続」
- 「US300c情報の表示」
- 「Internet Explorerによるインターネット閲覧」
- 「リモートデスクトップ接続の確立」
- 「Ericom PowerTerm Terminal Emulationとの接続の管理」
- 「NeutronとのUS300cの日付時刻の同期」
- 「VMware View Clientによる仮想デスクトップへの接続」

[WinVNC Current User Properties]については、「WinVNC Current User Propertiesの設定」を参照してください。

Online plug-inを使用した接続

ユーザーおよび管理者は、Online plug-inを使用できます。Online plug-inアプリケーションは、ICAサーバー上で動作しているリモートアプリケーションへの接続に使用します。

Online plug-inアプリケーションを起動する場合は，[すべてのプログラム]→[Online plug-in]をクリックするか、デスクトップの[Online plug-in]アイコンをダブルクリックしてください。

ICAクライアントアプリケーションのマニュアルは、CitrixのWebサイト（http://www.wyse.com/products/software）で入手できます。

US300c情報の表示

ユーザーおよび管理者は、US300c情報を閲覧することができます。US300cの情報を表示するには、[Client Information]ダイアログボックスを使用します(ダイアログボックスに表示される情報は、US300cおよびソフトウェアリリースによって異なります)。

[Client Information]ダイアログボックスは[すべてのプログラム]→[このデバイスについて]で表示されます。
たとえば、[General]タブをクリックすると、Webサイト、製品名、製品ID、バージョン、Windows Embedded Standard のバージョン、イーサネットMACアドレス、ワイヤレスMACアドレス、シリアル番号、ターミナルハードウェアのリビジョン、CPUの種類、MHz単位のCPU速度、フラッシュメモリの設定、RAMの設定、システムパーティションなどのUS300c情報が表示されます。

以下のタブをクリックして、US300c情報をさらに表示することもできます。

- [Installed Modules]
  US300cにインストールされているアプリケーションのリストを表示します。
- [WDM Packages]
  US300cに適用されているWDMパッケージのリストを表示します(「Wyse Device Managerソフトウェアを使用したリモート管理」を参照してください)。
- [QFEs]
  US300cに適用されているMicrosoft QFE(旧ホットフィックス)のリストを表示します。
- [Copyrights/Patents]
  著作権および特許情報を表示します。

Internet Explorerによるインターネット閲覧

ユーザーおよび管理者は、Microsoft Internet Explorer 8を使用してインターネット閲覧が可能です。ブラウザには、出荷時に選択されているインターネットオプション設定があります。これはフラッシュメモリへの書き込みを制限し、使用可能フラッシュメモリを使い果たさないようにするための設定なので、変更しないでください。
ブラウザは、［すべてのプログラム］→［Internet Explorer］より起動します。
ブラウザリソースがさらに必要な場合は、ICAまたはRDPセッションを使用して別のブラウザにアクセスできます。

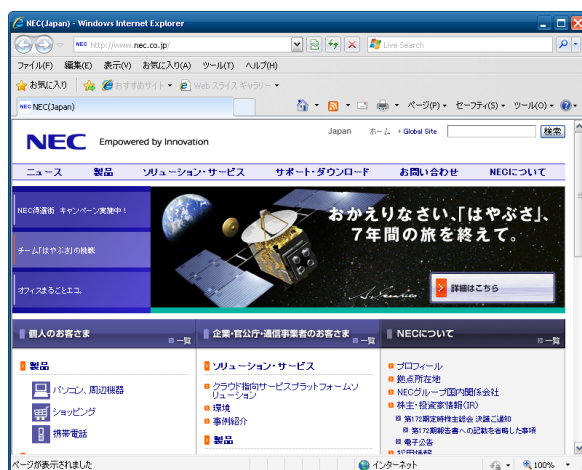



図6-1　Internet Explorer

リモートデスクトップ接続の確立

ユーザーおよび管理者は、リモートデスクトップ接続を使用できます。リモートアプリケーションへ接続し、管理します。
リモートデスクトップ接続を使用するには、［すべてのプログラム]→[リモートデスクトップ接続]をクリック、またはデスクトップの[リモートデスクトップ接続]アイコンをダブルクリックして[リモートデスクトップ接続]ダイアログボックスを表示します。

シングルモニター表示には標準バージョン(デフォルト)を使用します。1つのセッションを2つのモニターに拡張するとき(デュアルモニター対応シンクライアントの場合)は、リモートデスクトップ接続(For Dual Moniter)を使用できます。FBWFキャッシュがフルになりつつある場合は、[エクスペリエンス]タブで[ビットマップのキャッシュ]を無効にできます。
リモートデスクトップ接続の使用方法については、Microsoft社のマニュアルを参照してください(http://www.microsoft.com)。

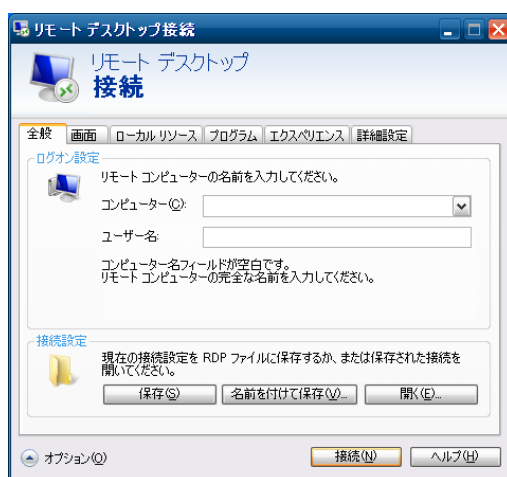



図6-2　リモートデスクトップ接続 - 拡張ビューの例

Ericom PowerTerm® Terminal Emulationとの接続の管理

ユーザーおよび管理者は、PowerTerm Session ManagerおよびPowerTerm Emulationを使用できます。

接続を管理するには、PowerTerm Session Managerを使用してください。

PowerTerm Session Managerは［すべてのプログラム］→[Ericom - PowerTerm® Terminal Emulation]→[PowerTerm Session Manager]より起動します。

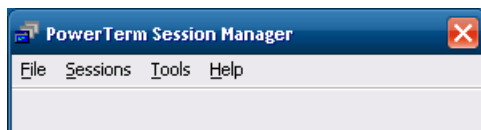



図6-3　Ericom社のPowerTerm® Session Manager

接続情報を設定するには、[TEC]ウィンドウおよび[Connect]ダイアログボックスを使用してください。

[TEC]ウィンドウおよび[Connect]ダイアログボックスは［すべてのプログラム］→[Ericom - PowerTerm® Terminal Emulation]→[PowerTerm Terminal Emulation]）より表示します。

Ericom社のPowerTerm® TECの全体的なインストールおよび使用手順については、Ericom PowerTerm® TECのマニュアルを参照してください。

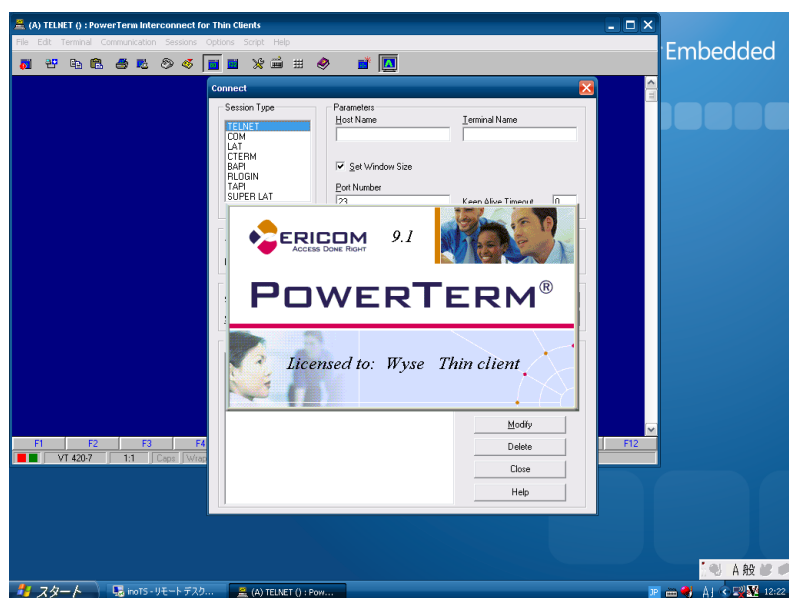



図6-4　Ericom社のPowerTerm® TECおよび[Connect]ウィンドウ

NeutronによるUS300cの日付時刻の同期

ユーザーおよび管理者は、Neutronによる日付時刻の同期を行えます。

[Neutron]ダイアログボックスは[すべてのプログラム]→[Neutron]より表示します。

[Neutron]ダイアログボックスには現在のシステム時刻および原子時が表示されています。
システム時刻を原子時に同期する場合は[Synchronize]をクリックしてください。
現在の原子時をタイムサーバーから取得するには、[Get Atomic Time]をクリックします。
ダイアログボックスの拡張メニューを開くには、[>>]をクリックします。

タイムサーバーと同期できない場合は、60秒後に終了し「Neutron could not synchronize the clock.Check network availability and connectivity with time server.」というメッセージを表示します。

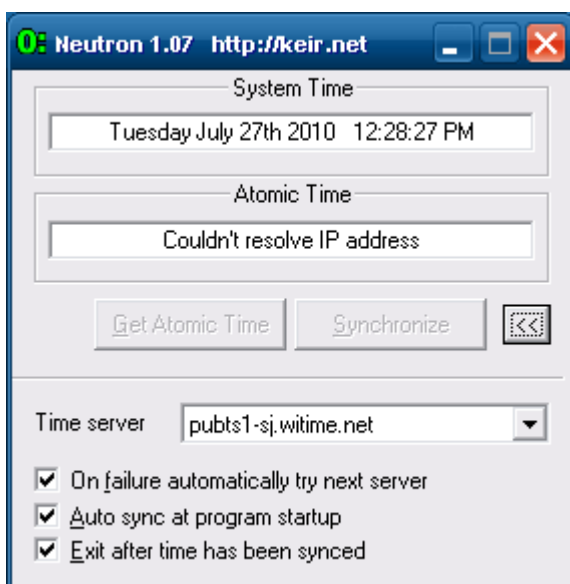



図6-5 Neutron - 拡張ビュー

VMware View Clientによる仮想デスクトップへの接続

ユーザーおよび管理者は、VMware View Clientを使用できます。仮想デスクトップに接続するには、[VMware View Client]ダイアログボックスを使用します。

[VMware View Client]ダイアログボックスは[すべてのプログラム]→[VMware]→[VMware View Client]より表示します。

ダイアログボックスの拡張メニューを開くには、[オプション(O) >>] をクリックします。

図6-6　VMware View Client - 拡張ビュー

以下のガイドラインに従ってください。

1. [Connection Server]ドロップダウンメニューでView Connection Serverのホスト名またはIPアドレスを入力し、[接続(C)]をクリックします。
2. 使用権限のあるユーザーの名前およびパスワードを入力し、ドメインを選択し、[Login]をクリックします。
3. 表示されるリストからデスクトップを選択し、[Connect]をクリックします。VMware View Clientが指定されたデスクトップへの接続を試みます。接続後、クライアントウィンドウが表示されます。

VMware View Clientの使用方法については、VMwareのWebサイトを参照してください(http://www.vmware.com)。

内蔵ワイヤレス機能の設定

オプションの内蔵ワイヤレス機能の設定は、Windowsワイヤレスゼロコンフィギュレーションユーティリティ(「ワイヤレスゼロコンフィギュレーション(WZC)の使用方法」を参照)を使用して行います。認証モードとして、Open、Shared、WPA、およびWPA2をサポートしています。

ワイヤレスゼロコンフィギュレーション(WZC)の使用方法

ここに示す手順を使用する前に、必要なユーザー証明書および(サーバーの)コンピュータ証明書がすべてUS300cにインポート済みであることを確認してください。

WZCを使用してオプションの内蔵ワイヤレス機能を設定するには、以下の手順を実行します。

1. [ネットワーク接続]ダイアログボックスを開き([スタート]→[コントロールパネル]→[ネットワーク接続])、利用可能なネットワーク接続を表示します。

2. [ワイヤレスネットワーク接続]を右クリックして[プロパティ]を選択し、[ワイヤレスネットワーク接続のプロパティ]ダイアログボックスを表示します。

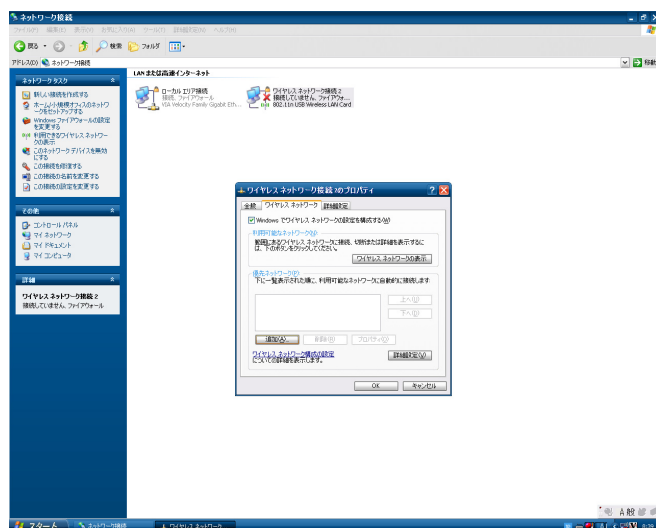



図6-7 [ワイヤレスネットワーク接続のプロパティ]

3. [ワイヤレスネットワーク]タブを選択し、[Windowsでワイヤレスネットワークの設定を構成する]のチェックボックスを選択します。

4. [OK]をクリックし、「EAP-TLS認証(スマートカードまたはその他の証明書)のためのワイヤレスシンクライアントの設定」または「PEAP-MS-CHAP v2向けのワイヤレスシンクライアントの設定」を参照して手順を続行します。

EAP-TLS認証(スマートカードまたはその他の証明書)のためのワイヤレスシンクライアントの設定

1. [ワイヤレスネットワーク接続]を右クリックして[プロパティ]を選択し、[ワイヤレスネットワーク接続のプロパティ]ダイアログボックスを表示します。

2. [ワイヤレスネットワーク]タブを選択して[追加(A)]をクリックし、[ワイヤレスネットワークのプロパティ]ダイアログボックスを表示します。

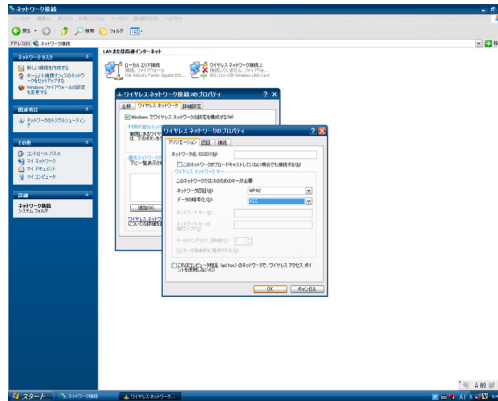



図6-8 [ワイヤレスネットワークのプロパティ] - EAP-TLS

3. [アソシエーション]タブをクリックします。

4. ネットワーク名(SSID)を入力します。

5. [ネットワーク認証]で[WPA2]オプションを選択します。

6. [データの暗号化]で[AES]オプションを選択します。

7. [認証]タブをクリックします。

8. [このネットワークで IEEE 802.1X 認証を有効にする]チェックボックスを選択します。

9. [EAP の種類]で[Smart Card or other Certificate]オプションを選択します。

10. [プロパティ]をクリックし、[スマートカードまたはほかの証明書のプロパティ]ダイアログボックスを表示します。

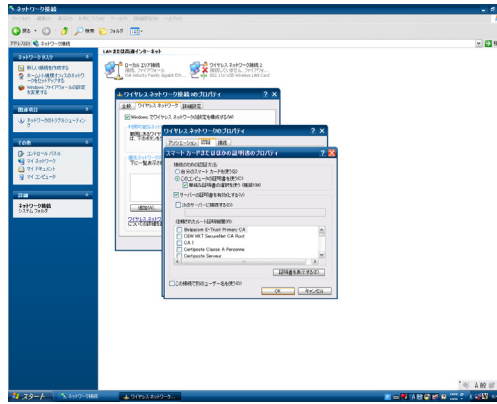



図6-9　[Smart Card or other Certificate Properties] - EAP-TLS

11. （レジストリベースのユーザー証明書を使用するために）［このコンピュータの証明書を使う］オプションを選択し、［単純な証明書の選択を使う］チェックボックスを選択します。

12. IASサーバーのコンピュータ証明書の有効性を確認するかどうかによって、［サーバーの証明書を検証する］チェックボックスを選択するか、または選択を解除します。チェックボックスを選択する場合は、［信頼されたルート証明機関］リストから（US300cに既にインポート済みの）必要な証明書を選択し、［OK］をクリックします。

13. すべての変更を保存し、すべてのダイアログボックスを閉じるまで［OK］をクリックします。

これでワイヤレス接続が確立されました。ワイヤレス接続が確立されていない場合は、以下のガイドラインに従ってください。

1. ［ネットワーク接続］ダイアログボックスを開き（［スタート］→［コントロールパネル］→［ネットワーク接続］）、利用可能なネットワーク接続を表示します。

2. ［ワイヤレスネットワーク接続］を右クリックして［利用できるワイヤレスネットワークの表示］を選択し、［ワイヤレスネットワーク接続］ダイアログボックスを表示します。

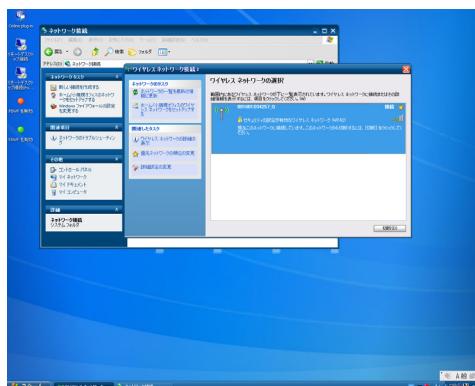



図6-10　［ワイヤレスネットワーク接続］ - EAP-TLS

3. 手順4で作成した接続（［ネットワーク名（SSID）］）を選択し、［接続］をクリックします。

これでワイヤレス接続が確立されました。

PEAP-MS-CHAP v2向けのワイヤレスシンクライアントの設定

1. [ワイヤレスネットワーク接続]を右クリックして[プロパティ]を選択し、[ワイヤレスネットワーク接続のプロパティ]ダイアログボックスを表示します。

2. [ワイヤレスネットワーク]タブを選択して[追加]をクリックし、[ワイヤレスネットワークのプロパティ]ダイアログボックスを表示します。

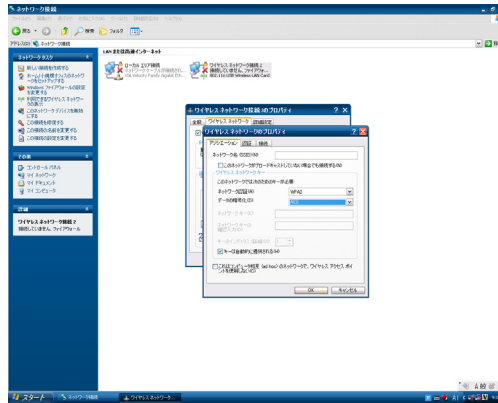



図6-11　[ワイヤレスネットワークのプロパティ] - PEAP-MS-CHAP v2

3. [アソシエーション]タブをクリックします。

4. ネットワーク名(SSID)を入力します。

5. [ネットワーク認証]で[WPA2]オプションを選択します。

6. [データの暗号化]で[AES]オプションを選択します。

7. [認証]タブをクリックします。

8. [このネットワークで IEEE 802.1X 認証を有効にする]チェックボックスを選択します。

9. [EAP の種類]で[Protected EAP (PEAP)]オプションを選択します。

10. [プロパティ]をクリックし、[保護されたEAPのプロパティ]ダイアログボックスを開きます。

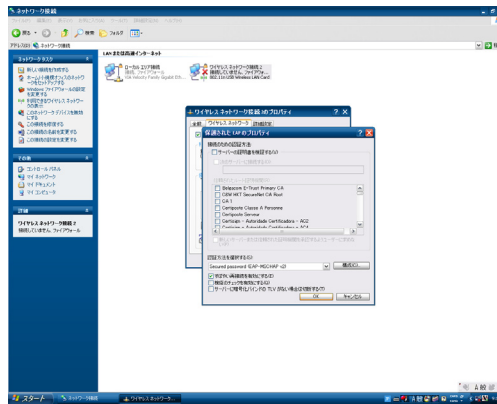



図6-12　[Protected EAP Properties] - PEAP-MS-CHAP v2

11. ［サーバーの証明書を検証する］チェックボックスの選択を解除します。

12. ［すばやい再接続を有効にする］チェックボックスを選択します。

13. ［構成］をクリックし、［EAP MSCHAPv2 のプロパティ］ダイアログボックスを開きます。

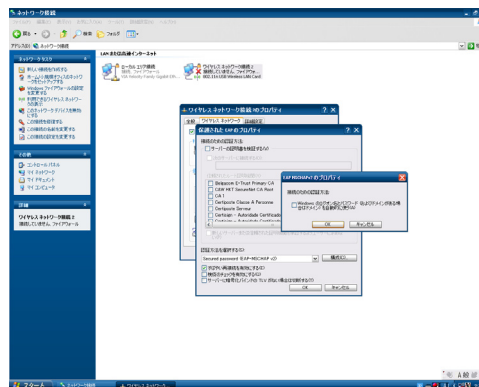



図6-13　[EAP MSCHAPv2 Properties] - PEAP-MS-CHAP v2

14. ［Windows のログオン名とパスワード（およびドメインがある場合はドメイン）を自動的に使う］チェックボックスの選択を解除し、［OK］をクリックします。

15. ［OK］をクリックします。認証情報の入力を求められます。

16. システムトレイに表示される「ワイヤレスネットワーク接続」ポップアップメッセージをクリックし、［資格情報の入力］ダイアログボックスを表示します。

17. 手順4で作成した接続（［ネットワーク名（SSID）］）を選択し、［接続］をクリックします。

18. システムトレイに表示される「ワイヤレスネットワーク接続」ポップアップメッセージをクリックし、［資格情報の入力］ダイアログボックスを表示します。

図6-14　[Enter Credentials] - PEAP-MS-CHAP v2

19. ユーザー名、パスワード、ドメイン名を入力し、[OK]をクリックします。

これでワイヤレス接続が確立されました。

ワイヤレス接続の保存

Windows Embedded Standardには、Write Filter Enable モードでワイヤレスアクセスを設定するための、Regpersistence.exeというツールがあります。このユーティリティを使用してワイヤレスアクセスを設定すると、リブートしても認証情報が維持されるので、US300cを再起動する度に再認証する必要がなくなります。このユーティリティは、ワークグループモード間およびドメイン間のワイヤレス接続用のサービスセットID(SSID)を保存します。Windows Embedded Standardクライアントは、再起動時、目的のワイヤレスアクセスポイントに自動的に接続されます。

Windows Embedded Standardクライアントは、以下のネットワーク認証モードを使用して、ワイヤレスネットワークに接続できます。

- WEPを使用するオープンモード

この認証モードでは、US300cがワイヤレスネットワークに接続している間にネットワークキーを入力する必要があります。Windows Embedded Standardクライアントは、リブート後、ワイヤレスネットワークに自動的に接続されます。

- WEPを使用する共有モード
- AESおよびTKIPを使用するWPA認証
- AESおよびTKIPデータ暗号化を使用するWPA-PSK
- AESおよびTKIPデータ暗号化を使用するWPA2
- AESおよびTKIPデータ暗号化を使用するWPA2-PSK
- PEAP認証プロセス

PEAP認証プロセス中に生成されるセッション鍵は、ワイヤレスクライアントとワイヤレスアクセスポイント間で送受信されるデータを暗号化するWEP(Wired Equivalent Privacy)暗号鍵の鍵材料を提供します。

PEAPは、ワイヤレス認証のための以下の認証方法のいずれとも使用できます(EAP-MD5との使用はサポートされていません)。

- サーバーの認証に証明書を、ユーザーおよびクライアントコンピュータの認証に証明書またはスマートカードを使用するEAP-TLS
- サーバーの認証に証明書を、ユーザーの認証に認証情報を使用するEAP-MS-CHAP v2
- Microsoft以外のEAP認証方法

PEAPは802.11ワイヤレスクライアントの認証方法として使用できますが、仮想プライベートネットワーク(VPN)クライアントやその他のリモートアクセスクライアントではサポートされていません。このため、インターネット認証サービス(IAS)を使用している場合のみ、リモートアクセスポリシーの認証方法としてPEAPを設定できます。

PEAP高速再接続の使用

US300 c が802.11ワイヤレスネットワークに接続するときには、認証済みセッションの期間を限定するためにネットワーク管理者が有効期限の間隔を認証済みセッションに設定します。認証済みのUS300cがセッションを定期的に再認証して再開する必要がないように、高速再接続オプションを有効にすることができます。

各ワイヤレスアクセスポイントが同じIAS(RADIUS)サーバーのクライアントとして設定されている場合のみ、PEAPによる高速再接続が可能です。高速再接続は、ワイヤレスクライアントとRADIUSサーバーの両方で有効にする必要があります。

PEAP高速再接続が有効になると、最初のPEAP認証に成功した後、クライアントおよびサーバーはTLSセッション鍵をキャッシュに保存します。ユーザーが新しいワイヤレスアクセスポイントに関連付けられると、クライアントおよびサーバーは、キャッシュの有効期限が切れるまで、キャッシュに保存した鍵を使用して互いに再認証します。鍵はキャッシュに保存されるので、RADIUSサーバーは、クライアント接続が再接続であることをすばやく判断できます。このため、クライアントによる認証要求とRADIUSサーバーによる応答間の遅延を短縮できます。クライアントおよびサーバーに対するリソース要件も軽減されます。

セッション鍵をキャッシュに保存したRADIUSサーバーを使用しない場合は、完全な認証が必要で、認証情報またはPINが再度求められます。この状況になる可能性があるのは、以下のような場合です。

- 別のRADIUSサーバーのクライアントとして設定されている新しいワイヤレスアクセスポイントにユーザーを関連付ける場合
- ユーザーを関連付けるワイヤレスアクセスポイントは同じだが、ワイヤレスアクセスポイントが別のRADIUSサーバーに認証要求を転送する場合

どちらの状況でも、新しいRADIUSサーバーとの最初の認証に成功した後、クライアントは新しいTLSセッション鍵をキャッシュに保存します。クライアントは、複数のRADIUSサーバーのTLSセッション鍵をキャッシュに保存できます。

7 管理ユーティリティと設定

管理ユーティリティと設定について説明しています。

管理者用コントロールパネルの拡張オプションの利用

このセクションでは、管理者用コントロールパネル内の拡張機能([スタート]→[コントロールパネル]から使用できるオプション)の概要を紹介します。

以下の項目について説明します。

- 「管理ツールへのアクセスと管理ツールの使用方法」
- 「カスタムフィールドによる設定文字列の設定」
- 「デュアルモニター表示の設定」
- 「Dual Video VGA RAMの設定」
- 「プリンタの設定」
- 「RAMディスクサイズの設定」
- 「地域と言語のオプションの選択」
- 「サウンドとオーディオデバイスの管理」
- 「WDMプロパティの設定」
- 「Winlogによる自動ログオンの有効/無効化」

FTP Addon Installerについては、「FTP Addon Installerを使用したアドオンのインストールとアップグレード」を参照してください。

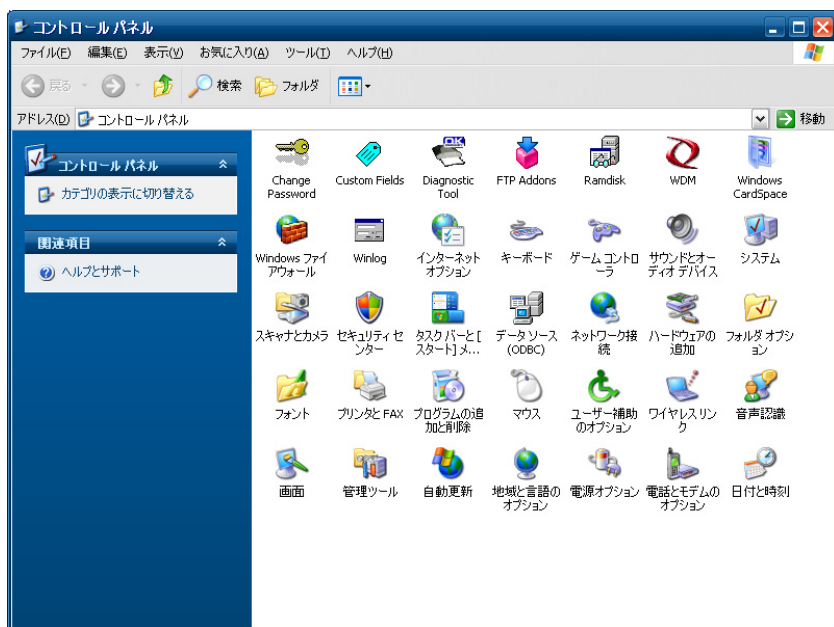



図7-1 管理者用コントロールパネルの例

管理ツールへのアクセスと管理ツールの使用

コントロールパネルの[管理ツール]アイコンをダブルクリックすると、[管理ツール]ウィンドウが表示されます。

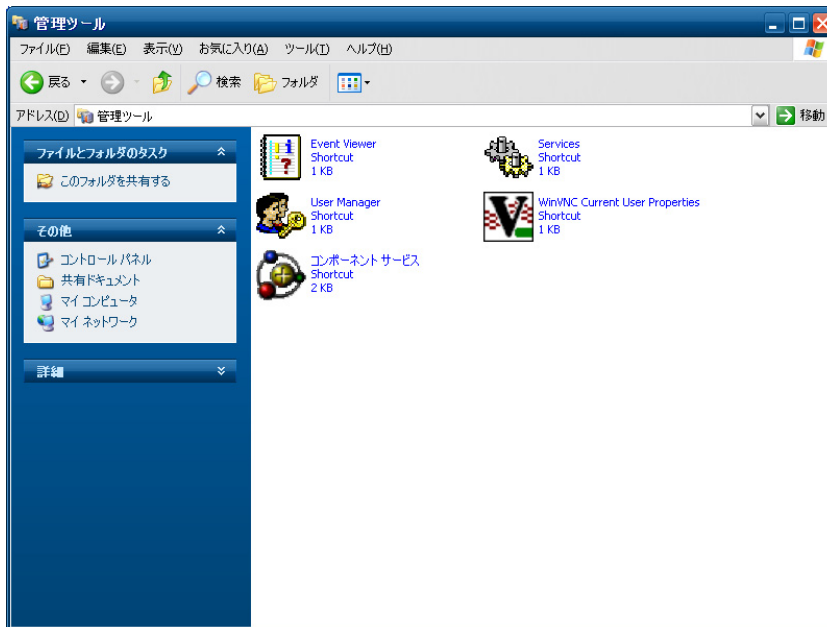



図7-2　[管理ツール]

管理ツールでは、以下の項目を設定できます。

- 「コンポーネントサービスの設定」
- 「イベントの表示」
- 「サービスの管理」
- 「ユーザーの管理」
- 「WinVNC Current User Propertiesの設定」

コンポーネントサービスの設定

［コンポーネントサービス］アイコンをダブルクリックすると、［コンポーネントサービス］ウィンドウが表示されます。コンソールでは、［コンポーネントサービス］、［イベント ビューア（ローカル）］、［サービス（ローカル）］の各項目を設定することができます。

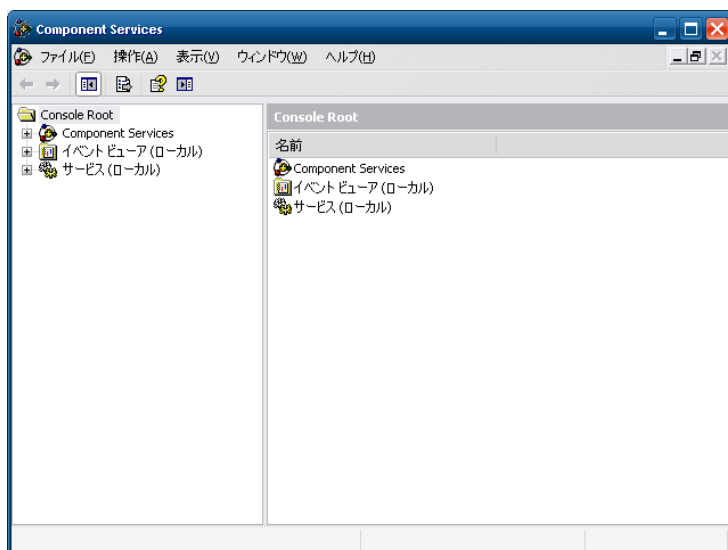



図7-3　［コンポーネントサービス］

イベントの表示

［イベントビューア］アイコンをダブルクリックすると、［イベントビューア］ウィンドウが表示されます。このツールは、Windowsや他のプログラムからの監視およびトラブルシューティングメッセージを表示します。

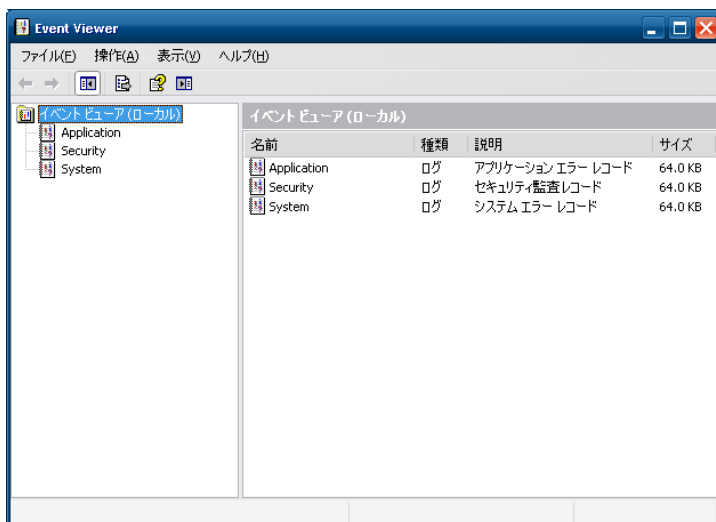



図7-4　［イベントビューア］

サービスの管理

[サービス]アイコンをダブルクリックすると、[サービス]ウィンドウが表示されます。このウィンドウには、US300cにインストールされているサービスが一覧表示されます。VNC ServerとClient Cleanup (NetXClean)は、US300c管理者が停止または再起動する必要がある場合があります。これらのサービスについては、「管理ユーティリティと設定」を参照してください。

VNC ServerとClient Clean-up(NetXClean)は、タスクマネージャから停止できます。

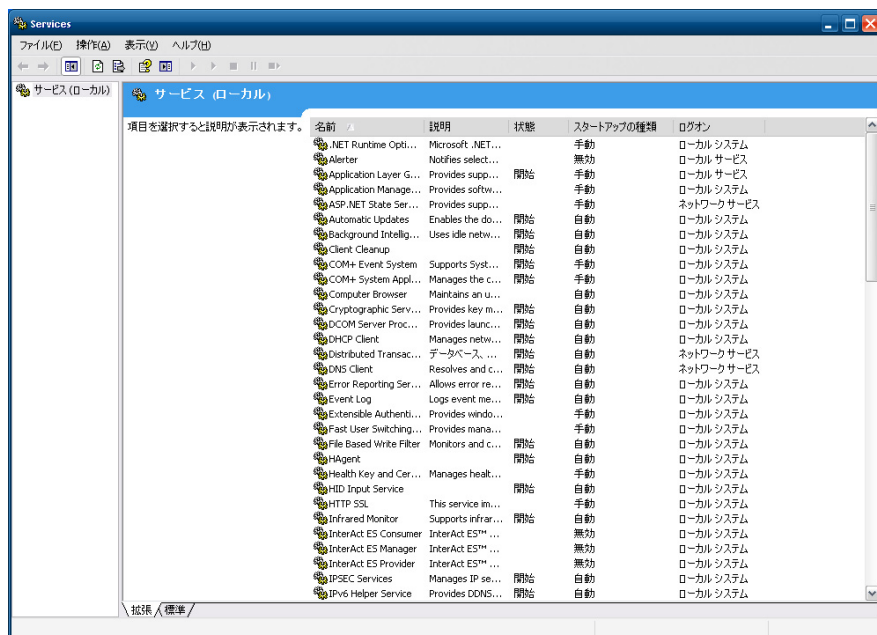



図7-5 [サービス]

ユーザーの管理

［ユーザーマネージャ］アイコンをダブルクリックすると、［ローカルユーザーとグループ］ウィンドウが表示されます。このツールを使用して、管理者はユーザーおよびグループを管理できます。ユーザーマネージャについては、「ユーザーマネージャによるユーザーとグループの管理」を参照してください。

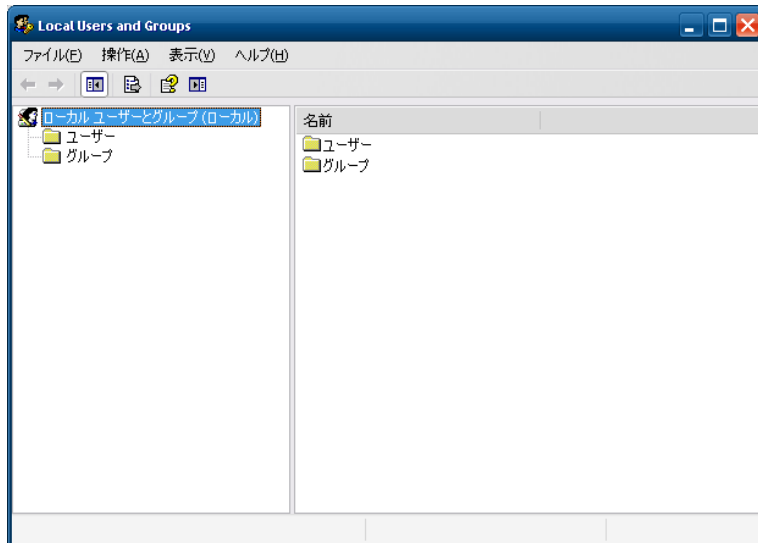



図7-6 ［ローカルユーザーとグループ］

WinVNC Current User Propertiesの設定

[WinVNC Current User Properties]アイコンをダブルクリック(または[すべてのプログラム]→[WinVNC Current User Properties]をクリック、またはシステムトレイ内のアイコンをダブルクリック)すると、[TightVNC Server: Current User Properties]ダイアログボックスが表示されます。このダイアログボックスは、VNCログオンパスワード(デフォルトでは「NEC」)を入力したり、US300cにインストールされているVNC Serverユーティリティのパラメータを選択するために使用します。

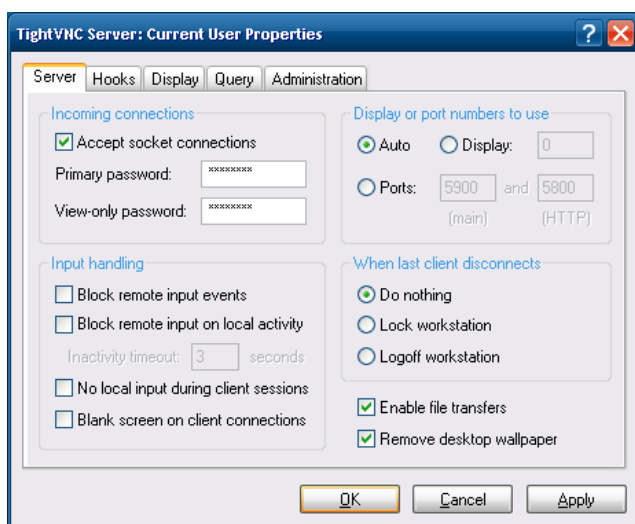



図7-7 [TightVNC Server: Current User Properties]

VNC Serverを使用して、VNC ViewerがインストールされているリモートマシンからUS300cを操作および監視(リモートシャドー)できます。VNCの主な目的はサポートとトラブルシューティングです。VNCユーザー設定については、「WinVNCを使用したUS300cのリモートシャドー」を参照してください。

タスクバーの[TightVNC Server]アイコンの上にマウスポインタを置くと、US300cの現在のIPアドレスが表示されます。

カスタムフィールドによる設定文字列の設定

コントロールパネルの[Custom Fields]アイコンをダブルクリックすると、[Custom Fields]ダイアログボックスが表示されます。このダイアログボックスは、WDMソフトウェアが使用する設定文字列を入力するために使用します。文字列には、場所、ユーザー、管理者などの情報を設定することができます。

[OK]をクリックすると、ダイアログボックスで入力したカスタムフィールド情報がWindowsレジストリに転送されます。これにより、WDM Client Managerでこの情報を使用できるようになります。情報を永続的に保存するには、レジストリ項目を作成または変更するシステムセッション中に、FBWFキャッシュのファイルを一括書き込みします(「US300cの設定」を参照してください)。

WDMを使用したリモート管理およびUS300cソフトウェアのアップグレードについては、「Wyse Device Managerソフトウェアを使用したリモート管理」を参照してください。

カスタムフィールド情報の使用方法については、WDMのマニュアルを参照してください。

図7-8　[CustomFields]

デュアルモニター表示の設定

[画面のプロパティ]ダイアログボックスの[設定]タブを使用して、デュアルモニターの設定を行うことができます。
[画面のプロパティ]ダイアログボックスは管理者用コントロールパネルの[画面]アイコンをダブルクリックして表示します。

(http://www.microsoft.comにあるMicrosoft社のマニュアルを参照してください)。Wyse社のマルチディスプレイおよびデュアルモニターの対応については、Wyse社のWebサイトのWyseナレッジベースを参照してください。

図7-9　[画面のプロパティ]

N8120-107 デュアルモニター用スプリッターケーブル(オプション)を使用した時のみ設定可能です。
デュアルモニター設定を行う際には、必ず両方のモニターを同じ解像度に設定してください。

プリンタの設定

US300cには、ローカル接続プリンタへのテキストのみの印刷をサポートするための汎用プリンタドライバがインストールされています。ローカル接続プリンタにフルテキストおよびグラフィックを出力するには、メーカーから提供されているドライバを手順に従ってインストールします。このインストールを保存するには、FBWFキャッシュのファイルを一括書き込みする必要があります。一括書き込みの手順については、「File Based Write Filter（FBWF）の使用方法」を参照してください。

ICAまたはRDPアプリケーションからのネットワークプリンタへの出力は、サーバー上のプリンタドライバを使用して実行できます。

サーバーのプリンタドライバを使用してICAまたはRDPセッションからローカル接続プリンタに出力すると、このプリンタでのフルテキストおよびグラフィック機能が利用可能になります。この操作を実行するには、「プリンタの追加」の手順に従って、プリンタドライバをサーバーに、テキスト専用ドライバをUS300cにインストールします。

プリンタの追加

プリンタドライバをサーバーに、テキスト専用ドライバをUS300cにインストールするには、以下の手順を実行します。

1. プリンタをUS300cに接続します。
2. ［スタート］→［プリンタとFAX］をクリックし、［プリンタとFAX］ダイアログボックスを開きます。
3. ［プリンタの追加］をクリックしてプリンタの追加ウィザードを開き、［次へ］をクリックします。
4. ［このコンピュータに接続されているローカルプリンタ］を選択し、［プラグアンドプレイ対応プリンタを自動的に検出してインストールする］チェックボックスの選択を解除し、［次へ］をクリックします。
5. ［次のポートを使用］を選択し、リストからポートを選択し、［次へ］をクリックします。
6. プリンタのメーカーと機種を選択して［次へ］をクリックします。
7. プリンタの名前を入力して［次へ］をクリックします。
8. ［このプリンタを共有しない］を選択して［次へ］をクリックします。
9. テストページを印刷するかどうかを選択して［次へ］をクリックします。
10. ［完了］をクリックします（インストールが完了し、テストページ印刷オプションを選択した場合は、テストページが印刷されます）。

RAMディスクサイズの設定

RAMディスクは、一時的なデータ保存に使用される揮発性記憶空間です。[マイコンピュータ]ウィンドウでは、Zドライブと表示されます。RAMディスクは、管理者の判断により、他のデータの一時保存にも使用できます(「ファイルの保存とローカルドライブの使用方法」を参照してください)。

RAMディスクには以下のものが保存されます。

- ブラウザのWebページのキャッシュ
- ブラウザの履歴
- ブラウザのCookie
- ブラウザのキャッシュ
- インターネットテンポラリファイル
- 印刷スプーリング
- ユーザーとシステムのテンポラリファイル

コントロールパネルの[Ramdisk]アイコンをダブルクリックすると、[Ramdisk Configuration]ダイアログボックスが表示されます。このダイアログボックスを使用して、RAMディスクのサイズを設定します。RAMディスクのサイズを変更すると、システムを再起動して変更を有効にするように求められます。ただし、変更を永続的に保存するには、必ずシステムを再起動する前のカレントシステムセッション中にFBWFキャッシュのファイルを一括書き込みしてください(「US300cの設定」を参照)。

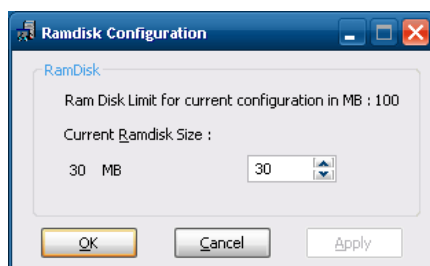



図7-10 [Ramdisk Configuration]

デフォルトのRAMディスクサイズは、US300cのモデルおよびインストールされているメモリのサイズによって異なる場合があります。設定可能な最小RAMディスクサイズは2 MBです。設定可能な最大RAMディスクサイズは、RAMが512 MB以下のシステムでは実際のRAMの約20%、RAMが512 MBを超えるシステムでは実際のRAMの約10%です(RAMが1 GB以上のシステムの場合、設定可能な最大RAMディスクサイズは100 MBに制限されます)。

地域と言語のオプションの選択

コントロールパネルの[地域と言語のオプション]アイコンをダブルクリックすると、〔地域と言語のオプション]ダイアログボックスが表示されます。このダイアログボックスを使用して、キーボードの言語を選択します。サポートされているキーボード言語を以下に示します。

アラビア語
オランダ語（ベルギー）
フランス語（ベルギー）
ブラジルポルトガル語(ABNT)+A34
英語（カナダ）（マルチ）
フランス語（カナダ）（マルチ）
フランス語（カナダ）
チェコ語
クロアチア語
デンマーク語
オランダ語
英語（英）
英語（米）
フィンランド語
フランス語
ドイツ語
ギリシャ語
ヘブライ語
ハンガリー語
イタリア語
イタリア語（142）
スペイン語（南米）
ノルウェー語
ポーランド語（214）
ポーランド語（プログラマ）
ポルトガル語
日本語（デフォルト）
ルーマニア語
ロシア語
スロバキア語
スロベニア語
スペイン語
スペイン語方言
スウェーデン語
フランス語（スイス）
ドイツ語（スイス）
タイ語
トルコ語-F
トルコ語-Q
米国国際

日本語以外のすべての言語では、言語に合ったキーボードが必要です。キーボードは、表内の言語ごとに異なります。

US300cに多言語ビルドが含まれており、別の言語に変更したい場合は、以下の手順を実行します。

1. 〔スタート〕→〔コントロールパネル〕をクリックします。
2. 〔地域と言語のオプション〕アイコンをダブルクリックし、〔地域と言語のオプション〕ダイアログボックスを開きます。
3. 〔言語〕タブをクリックします。
4. 〔メニューとダイアログで使われる言語〕リストから言語を選択し、〔適用〕をクリックします（ログオフして再度ログオンするまで変更は有効にならないというメッセージが表示されます ）。
5. 〔OK〕をクリックします。
6. 〔地域と言語のオプション〕ダイアログボックスで[OK]をクリックし、コントロールパネルを閉じます。
7. 現在のユーザーをログオフします。
8. US300cにログオンします（GUIが選択した言語で表示されます）。

サウンドとオーディオデバイスの管理

[サウンドとオーディオデバイス]アイコンをダブルクリックすると、[サウンドとオーディオデバイス]ダイアログボックスが表示されます。このダイアログボックスを使用して、音声およびオーディオデバイスを管理します。タスクバーのシステムトレイ内にある[音量]アイコンを使用して音量を調節することもできます。[音量]アイコンをクリックすると、マスター音量コントロールが開きます。ダブルクリックすると、Volume Controlアプリケーションのダイアログボックスが開きます。

WDMプロパティの設定

コントロールパネルの[WDM]アイコンをダブルクリックすると、[WDM Properties]ダイアログボックスが表示されます。このダイアログボックスを使用して、WDMの設定を行います。

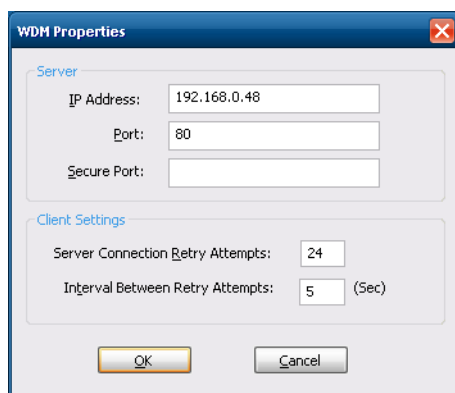



図7-11　[WDM Properties]

以下のガイドラインに従ってください。

1. WDMサーバーのIPアドレスまたはホスト名を入力します。
2. 使用するポートを入力します。
3. [OK]をクリックします。

WDMソフトウェアについては、「Wyse Device Managerソフトウェアを使用したリモート管理」を参照してください。

Winlogによる自動ログオンの有効／無効化

US300cのデフォルトでは、ユーザーデスクトップへの自動ログオンが有効になっています。コントロールパネルの[Winlog]アイコンをダブルクリックすると、[Winlog]ダイアログボックスが表示されます。このダイアログを使用して、自動ログオンを有効または無効にし、US300cに自動ログオンするユーザー名、パスワード、およびドメインを変更します。

US300cで行った設定（自動ログオンのプロパティなど）をUS300cのリブート後も維持するには、「US300cの設定」で説明しているように、必ずUS300cの設定変更の前にFBWFを無効にし、設定変更後に再度有効にしてください。FBWFについては、「File Based Write Filter（FBWF）の使用方法」を参照してください。

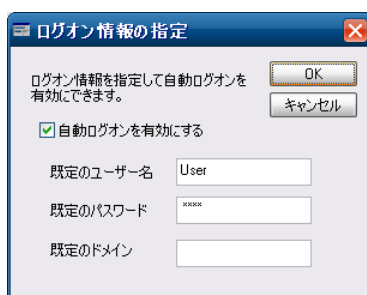



図7-12　Winlog

File Based Write Filter(FBWF)の使用方法

FBWFは、フラッシュメモリへの誤った書き込みからUS300cを保護することにより、US300cでのコンピュータ処理にセキュアな環境を提供します(フラッシュメモリには、オペレーティングシステムおよび機能ソフトウェアコンポーネントが格納されています)。FBWFは過度のフラッシュ書き込み動作を防止するため、US300cの寿命も長くなります。FBWFは、キャッシュを使用してすべてのフラッシュ書き込みを遮断し、入出力を要求したプロセスに正常終了メッセージを返すことで、フラッシュへのリード/ライトアクセスが行われているように見せます。

遮断されキャッシュに保存されたフラッシュ書き込みは、US300 c がアクティブな状態である限り使用できますが、US300cを再起動またはシャットダウンすると失われます。選択した変更を保存するには、WDMソフトウェアを使用するかまたは手動で、[File Based Write Filter Control]ダイアログボックス(管理者タスクバーのシステムトレイ内に表示されているFBWFアイコンをダブルクリック)の[Commit]を使用して、キャッシュ内の選択したファイルを必要に応じてフラッシュに転送します。また、変更により影響を受けるファイルが不明な場合は、[File Based Write Filter Control]ダイアログボックスでFBWFをいったん無効にした後で変更を行い、変更後、FBWFを再度有効にすることもできます(「FBWFのコントロールの設定」を参照してください)。FBWFは、コマンドライン(fbwfmgr)を使用するか、管理者システムトレイの[File Based Write Filter]アイコンをダブルクリック、またはデスクトップの[FBWF を有効 /FBWF を無効]アイコンを使用して、有効または無効にすることができます。FBWFの状態(有効または無効)は、システムトレイの[File Based Write Filter]アイコンによって表示されます(緑はFBWFが有効なことを示し、赤はFBWFが無効なことを示します)。FBWFは、キャッシュからフラッシュに指定のファイルを一括書き込みできます(コミット処理が実行される時点まで。一括書き込みしたファイルに対してさらに書き込みを行った場合、追加した変更も保存する必要があるときは、これらのファイルを再度一括書き込みしてコミットする必要があります)。

80%以上データが入っている場合は、絶対にFBWFキャッシュの内容を一括書き込みしないでください。管理者は、キャッシュの状態を定期的にチェックし、キャッシュに80%以上データが入っている場合はUS300cを再起動する必要があります。

ターミナルサービスクライアントアクセスライセンス(TSCAL)は、FBWFの有効/無効にかかわらず常に保持されます。
FBWFの有効/無効にかかわらず他のレジストリ設定を保存する場合は、「Wyseの技術サポート 」を参照し、Wyseのサポート部門 にお問い合わせください。

FBWFの使用については、以下のセクションを参照してください。

- 「FBWFによるパスワードの変更」
- 「FBWFコマンドラインオプションの実行」
- 「デスクトップアイコンによるFBWFの有効/無効化」
- 「FBWFのコントロールの設定」

FBWFによるパスワードの変更

Microsoft Windows NTベースのコンピュータおよびMicrosoft Windows 2000または2003ベースのコンピュータでは、セキュリティ上、ドメインコントローラを使用してマシンアカウントパスワードを定期的に変更します。Windows NTベースのコンピュータでは、マシンアカウントパスワードはデフォルトで7日ごとに自動的に変更されます。Windows 2000または2003ベースのコンピュータでは、マシンアカウントパスワードは30日ごとに自動的に変更されます。

US300cがこのようなドメインのメンバーの場合は、同じパスワード処理がUS300cに適用されます。FBWFが有効な場合、US300cはドメインコントローラでこのパスワードを正常に変更します。ただし、FBWFが有効なため、次回ブート時、US300cは新しいパスワードを保持しません。このような場合は、以下の選択肢があります。

- DisablePasswordChangeレジストリ項目に「1」を設定し、US300cでのマシンアカウントパスワードの変更を無効にする。
- 各ワークステーションの代わりに、ドメイン内のすべてのドメインコントローラでRefusePasswordChangeレジストリ項目に「1」を設定し、Windows NT 4.0、Windows 2000、2003でのマシンアカウントパスワードの変更を無効にする。上記設定後も、US300cは30日ごとにパスワードを変更しようとしますが、サーバーによって拒絶されます。

Windows NT 4.0ドメインコントローラでは、プライマリドメインコントローラ(PDC)で変更を加える前に、ドメイン内のすべてのバックアップドメインコントローラ(BDC)でRefusePasswordChangeレジストリ項目に「1」を設定する必要があります。この順序に従わないと、PDCのイベントログにイベントID 5722が記録されます。
Windows 2000または2003のドメインコントローラでRefusePasswordChangeレジストリ項目に「1」を設定すると、複製トラフィックは停止されますが、US300cのトラフィックは停止されません。US300cでDisablePasswordChangeレジストリ項目にも「1」を設定すると、US300cと複製の両方のトラフィックが停止されます。

US300cでのマシンアカウントパスワード変更の無効化

US300cでのマシンアカウントパスワードの変更を無効にするには、以下の手順を実行します。

1. レジストリエディタを起動するには、[スタート]→[ファイル名を指定して実行]をクリックして、[名前]テキストボックスに「regedit」と入力し、[OK]をクリックします。
2. 以下のレジストリサブキーの場所を探し、クリックします。
   HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Netlogon¥Parameters
3. 右のペインで、disablepasswordchangeを右クリックします。
4. [編集]メニューで[修正]をクリックします。
5. [値のデータ]テキストボックスに「1」を入力し、[OK]をクリックします。
6. レジストリエディタを終了します。

Windows NT 4.0、Windows 2000、2003でのマシンアカウントパスワード変更の無効化

Windows NT 4.0、Windows 2000、2003でのマシンアカウントパスワードの変更の無効にするには、以下の手順を実行します。

1. レジストリエディタを起動するには、[スタート]→[ファイル名を指定して実行]をクリックして、[名前]テキストボックスに「regedit」と入力し、[OK]をクリックします。
2. 以下のレジストリサブキーの場所を探し、クリックします。

   HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Netlogon¥Parameters
3. 右のペインの何も表示されていないエリアで、右クリックします。
4. [編集]メニューで[新規]をポイントし、[DWORD値]をクリックします。
5. レジストリ項目名としてRefusePasswordChangeを入力し、[ENTER]をクリックします。
6. [編集]メニューで[修正]をクリックします。
7. [値のデータ]テキストボックスに「1」を入力し、[OK]をクリックします。
8. レジストリエディタを終了します。

FBWFコマンドラインオプションの実行

FBWFのコントロールに使用できるコマンドラインは複数あります(コマンドラインの引数を組み合わせることはできません)。

これらのコマンドの不正使用を防止するためにNTファイルセキュリティを使用してください。

FBWFのコマンドラインオプションについては、以下のガイドラインに従ってください([スタート]→[ファイル名を指定して実行]をクリックして、[名前]テキストボックスに「command」と入力してコマンドプロンプトウィンドウを開き、コマンドを使用することもできます)。

チェック

コマンドプロンプトウィンドウを開いて「fbwfmgr /」と入力すると、使用可能なコマンドがすべて表示されます。コマンドの情報が知りたい場合は、fbwfmgr /help <command>を実行してください。たとえば、/addvolumeの情報が知りたい場合は、「fbwfmgr /help /addvolume」と入力します。

- fbwfmgr

  引数なし - カレントセッションおよび次のセッションのFBWF設定を表示します。

- fbwfmgr /enable

  次回システムを再起動した後にFBWFを有効にします。FBWFが有効な場合、[File Based Write Filter]アイコンは緑です。

- fbwfmgr /disable

  次回システムを再起動した後にFBWFを無効にします。FBWFが無効な場合、[File Based Write Filter]アイコンは赤です。

- fbwfmgr /commit C: <file_path>

  ファイルに加えた変更を基本メディアにコミットします。ボリューム名とfile_pathの間にスペースが1つ入っていることに注意してください。ファイルパス(file_path)には¥で始まる絶対パスを入力します。たとえば、ファイルC:¥Program Files¥temp.txtをコミットする場合、コマンドはfbwfmgr /commit C: "¥Program Files¥temp.txt"となります。

- fbwfmgr /restore C: <file_path>

  ファイルに加えた変更を破棄し、基本メディアから元の内容にファイルを復元します。ファイルパス(file_path)には¥で始まる絶対パスを入力します。削除されたファイルは回復されます。

- fbwfmgr /addexclusion C: <file_or_dir_path>

  ボリュームの除外リストにファイルまたはディレクトリを追加します。その結果、ファイルまたはディレクトリはFBWFの保護から外れます。除外は、次回のシステムリブート後有効になります。ファイルまたはディレクトリパス(file_or_dir_path)には、¥で始まる絶対パスを入力します。

- fbwfmgr /removeexclusion C: <file_or_dir_path>

  ボリュームの除外リストからファイルまたはディレクトリを削除します。その結果、ファイルまたはディレクトリはFBWFの保護下に置かれます。除外の解除は、次回のシステムリブート後有効になります。ファイルまたはディレクトリパス(file_or_dir_path)には、¥で始まる絶対パスを入力します。

- fbwfmgr /overlaydetail

  変更されたファイルおよびディレクトリのリストを、FBWFがファイルまたはディレクトリの変更データをキャッシュに保存するために使用するメモリのサイズとそれに対するオープンハンドルの数とともに表示します。

一括書き込みの実行中に一括書き込みを行わないでください。

デスクトップアイコンによるFBWFの有効／無効化

[FBWF を有効 / FBWF を無効]アイコンは、便宜上のため、管理者デスクトップにあります。これらのアイコンは、FBWFを有効または無効にするために使用します。

- **[FBWF を有効]アイコン**

  ダブルクリックすると、FBWFが有効になります。このユーティリティは、「FBWFコマンドラインオプションの実行」で説明しているfbwfmgr /enableコマンドラインオプションと同様の動作をします。ただし、このアイコンをダブルクリックすると、システムは自動で再起動され、FBWFが有効になります。FBWFが有効な場合、システムトレイの[File Based Write Filter]アイコンは緑です。

- **[FBWF を無効]アイコン**

  ダブルクリックすると、FBWFが無効になります。このユーティリティは、「FBWFコマンドラインオプションの実行」で説明しているfbwfmgr /disableコマンドラインオプションと同様の動作をします。ただし、このアイコンをダブルクリックすると、システムは自動で再起動され、FBWFが無効になります。FBWFは無効な状態を維持し、有効にするには、「FBWFコマンドラインオプションの実行」で説明しているように[FBWF を有効]アイコンかコマンドラインを使用します。FBWFが無効な場合、システムトレイの[File Based Write Filter]アイコンは赤です。

FBWFのコントロールの設定

[File Based Write Filter Control]ダイアログボックスは、管理者タスクバーのシステムトレイ内に表示されているFBWFアイコンをダブルクリックして表示します。

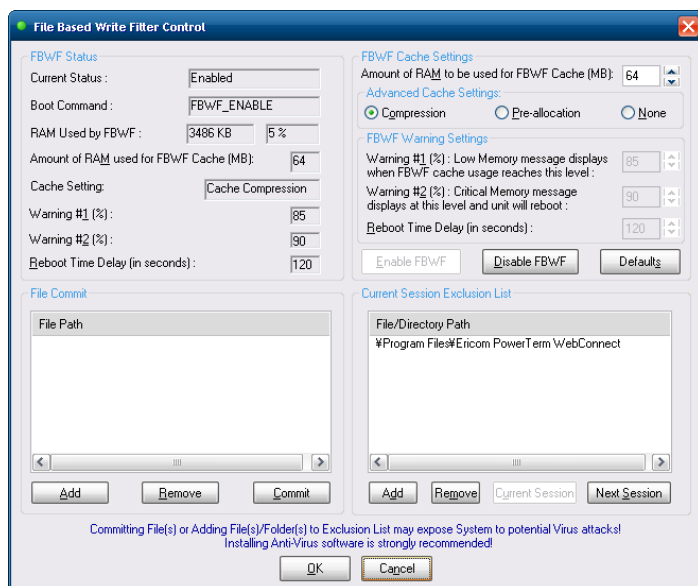



図7-13　[File Based Write Filter Control]

以下のガイドラインに従ってください。

- [FBWF Status]エリアには以下の項目があります。
  - **[Current Status]**

    FBWFの現在の状態(有効または無効)を表示します。
  - **[Boot Command]**

    Bootコマンドの現在の状態を表示します。(FBWF_ENABLEは、次のセッションではFBWFが有効になることを意味します。FBWF_DISABLEは、次のセッションではFBWFが無効になることを意味します)。
  - **[RAM Used by FBWF]**

    FBWFが現在使用しているRAMのサイズを、キロバイト単位およびパーセンテージで表示します。[Current Status]が[Disabled]の場合、[RAM Used by FBWF]は常にゼロ(0)です。
  - **[Amount of RAM used for FBWF Cache]**

    カレントセッションでFBWFキャッシュとして使用されているRAMのサイズをMB単位で表示します。
  - **[Cache Setting]**

    カレントセッションのキャッシュ設定を表示します。
  - **[Warning #1 (%)]**

    カレントセッションのユーザーに、メモリ残量の減少を警告するメッセージを表示させるFBWFキャッシュのパーセント値を表示します。
  - **[Warning #2 (%)]**

    ユーザーに、メモリ残量が限界まで枯渇していることを警告するメッセージを表示させるFBWFキャッシュのパーセント値と、同時に表示されるカレントセッションで自動リブートが行われるまでの秒数をカウントダウンするメッセージを表示します。
  - **[Reboot Time Delay (in seconds)]**

    カレントセッションでキャッシュオーバーフロー発生によりWarning #2 (%)のシステムリブートが実行されるまでの秒数を表示します。
- [FBWF Cache Settings]エリアには以下の項目があります。
  - **[Amount of RAM to be used for FBWF Cache]**

    次のセッションでFBWFキャッシュとして使用されるRAMのサイズをMB単位で表示します。この値は、16 MB～1024 MBの範囲である必要があります。この値が使用可能なRAMサイズの35%を上回っていないようチェックします。
- [Advanced Cache Settings]エリアには、キャッシュメモリの効率を高めるためのオプションがあります([Compression]、[Pre-allocation]、[None])。
- [FBWF Warning Settings]エリアには以下の項目があります。
  - **[Warning #1 (%)]**

    ユーザーにメモリ残量の減少を警告するメッセージを表示させるFBWFキャッシュのパーセント値を表示します(デフォルト値 = 85、最小値 = 50、最大値 = 90)。

- [Warning #2 (%)]

  ユーザーに、メモリ残量が限界まで枯渇していることを警告するメッセージを表示させるFBWFキャッシュのパーセント値と、同時に表示されるカレントセッションで自動リブートが行われるまでの秒数をカウントダウンするメッセージを表示します（デフォルト値 = 90、最小値 = 55、最大値 = 95）。

- [Reboot Time Delay (in seconds)]

  キャッシュオーバーフロー発生によりWarning #2 (%)のシステムリブートが実行されるまでの秒数を表示します。

● [Enable FBWF]

FBWFを有効にします。US300cの再起動を求められます。US300cを再起動後、変更が有効になります。FBWFを有効にするためにシステムを再起動すると、システムトレイの[File Based Write Filter]アイコンは緑になります。

● [Disable FBWF]

FBWFを無効にします。US300cの再起動を求められます。US300cを再起動後、変更が有効になります。FBWFを無効にするためにシステムを再起動すると、システムトレイの[File Based Write Filter]アイコンは赤になります。

● [Defaults]

[FBWF Cache Settings]エリア、[Advanced Cache Settings]エリア、および[FBWF Warning Settings]エリアをデフォルト値にリセットします。

● [File Commit]エリアには以下の項目があります。

- [File Path]

  ファイルを追加、削除、および基本メディアにコミットします（ファイルをコミットしない場合は、リストからファイルパスを削除します）。US300cは再起動されません。変更はただちにコミットされます。

● [Current Session Exclusion List]エリアには以下の項目があります。

- [File/Directory Path]

  現在の セッション（現在のセッションでライトスルーされるファイルまたはディレクトリのリストが表示されます。タイトルはCurrent Session Exclusion Listとなります）または次のセッション（次のセッションでライトスルーされるファイルまたはディレクトリのリストを取り出します。タイトルはNext Session Exclusion Listとなります）で除外リストにファイルまたはディレクトリを追加するか、除外リストからファイルまたはディレクトリを削除できます。

  クライアントは再起動されず、管理者がUS300cを手動で再起動するまで変更は反映されません。

NetXCleanユーティリティについて

NetXCleanは、無関係な情報がフラッシュメモリに保存されるのを防止します。NetXCleanは、バックグラウンドで実行されるサービスです。NetXCleanのクリーンアップは、サービスの起動またはユーザーによるログオフ時に自動的に実行されます。クリーンアップの実行はユーザーからは見えず、またユーザーは何も入力する必要はありません。

NetXCleanは、ガベージファイルの蓄積によりフラッシュメモリ内の容量が一杯になるのを防止します(たとえば、FBWFキャッシュ内のファイルを一括書き込みすると、クリーンな状態に保つ必要があるフラッシュディレクトリにゴミが溜まります)。複数のユーザーがUS300cへのログオン権を持っている場合、ローカルに保存されるプロファイルや情報の一時キャッシュによってメモリ容量をすぐに使い果たす可能性があるので、NetXCleanユーティリティは特に重要になります。

NetXClean TweakUI機能は、以下の項目を消去します。

- 実行履歴(ログオン時)
- 文書履歴(ログオン時)
- ファイル検索履歴(ログオン時)
- コンピュータ検索履歴(ログオン時)
- Internet Explorer履歴(ログオン時)
- 前回のユーザー(ログオン時)
- 現在選択されている項目

NetXCleanは、選択したディレクトリ、ファイル、およびプロファイルを消去します。また、設定ファイルに基づき、消去するディレクトリとファイル(および消去しないディレクトリとファイル)を判断します。消去する対象として別のディレクトリとファイルを選択するには、設定ファイルで該当ディレクトリとファイルを選択する必要があります。

重要

NetXCleanの消去する項目は、メーカーによって選択されています。メーカーによる指示なしに変更することはおやめください。

設定ファイルでの選択にかかわらず、NetXCleanは以下のディレクトリやその親ディレクトリを消去しません。

- Windowsディレクトリ
- Windows Systemサブディレクトリ
- サービスがインストールされているカレントディレクトリ

NetXCleanは、以下のプロファイルを消去しません。

- Administrator
- All Users
- Default User
- 前回ログオンしたユーザーのプロファイル

ファイルの保存とローカルドライブの使用方法

管理者は、ローカルドライブとファイルの保存について以下の情報を把握する必要があります。

ファイルの保存

US300cは、固定サイズのフラッシュメモリで、組み込みオペレーティングシステムを使用します。保持する必要があるファイルは、US300cではなくサーバーに保存することをお勧めします。

Cドライブに書き込みを行うフラッシュメモリ内アプリケーションの設定(特に、デフォルトでローカルシステムのCドライブにキャッシュファイルを書き込むアプリケーション)には注意してください。ローカルドライブに書き込む必要がある場合は、Zドライブを使用するようにアプリケーション設定を変更してください。
「ユーザーマネージャによるユーザーとグループの管理」で述べるデフォルト設定を使用すると、出荷時にインストールされているアプリケーションによるCドライブへの書き込みを最小限に抑えることができます。

FBWFについては、「File Based Write Filter(FBWF)の使用方法」を参照してください。

ドライブZ

ドライブZは、US300cのオンボード揮発性メモリ(Ms-ramdrive)です。保持する必要があるデータの保存には、このドライブは使用しないことをお勧めします。

RAMディスクの設定については、「RAMディスクサイズの設定」を参照してください。

Zドライブとローミングプロファイルの使用については、「ドメインへの参加」を参照してください。

ドライブCとフラッシュメモリ

ドライブCは、オンボード不揮発性フラッシュメモリです。ドライブCへの書き込みは避けることをお勧めします。ドライブCに書き込みを行うと、フラッシュメモリの空き容量が少なくなります。フラッシュメモリの空き容量が3 MBを下回ると、US300cの動作が不安定になります。

フラッシュメモリは3 MB分の空き容量を残すことを強くお勧めします。フラッシュメモリの空き容量が2 MBになると、US300cのイメージが修復不可能な状態まで破壊され、正規のサービスセンター に連絡してUS300cの修理が必要になります。

FBWFが有効な場合は、フラッシュメモリを破壊から保護し、キャッシュが上書きされるとエラーメッセージを表示します。ただし、このメッセージが表示されても、FBWFキャッシュのファイルを一括書き込みすることはできず、キャッシュ内に残っているUS300c設定の変更は失われます。
フラッシュメモリをクリーンな状態に維持するにあたってのNetXCleanの役割については、「NetXCleanユーティリティについて」を参照してください。

通常動作時にFBWFキャッシュに(FBWFが無効な場合はフラッシュメモリに直接)書き込まれる項目には、以下のようなものがあります。

- お気に入り
- 作成された接続
- 接続の削除と編集

ネットワークドライブのマッピング

ユーザーと管理者は、ネットワークドライブをマッピングできます。ただし、US300c再起動後もマッピングを保持するには、以下の手順を実行する必要があります。

- ［ログオン時に再接続する］チェックボックスを選択します。
- カレントシステムセッション中にFBWFキャッシュのファイルを一括書き込みします。

  ユーザーアカウントでログオンしている場合はFBWFキャッシュのファイルを一括書き込みできませんので、ユーザーアカウントをログオフし（システムのシャットダウンまたは再起動は行わないでください）、管理者アカウントで再度ログオンしてからキャッシュのファイルを一括書き込みすることにより、マッピングを保持できます。

ユーザーマネージャユーティリティを使用するか、または管理者が知っている別の方法によってリモートホームディレクトリを割り当てることもできます。

ドメインへの参加

US300cをドメインに参加させるか、ローミングプロファイルを使用することにより、ドメインに参加することができます。

ドメインへの参加

管理者は、[コンピュータ名の変更]ダイアログボックス([スタート]→[コントロールパネル]→[システム]→[コンピュータ名]タブ→[変更])で、US300cをドメインに参加させることができます。

ログオン時にダウンロードされるプロファイルによってキャッシュやフラッシュメモリがオーバーフローする場合があるので、ドメインにUS300cを参加させるときは特に注意が必要です。

US300cをドメインに参加させるときは、FBWFを無効にしてUS300cにドメイン情報を永続的に保存できるようにしてください。情報はドメイン参加後のブート時にUS300cに書き込まれるので、FBWFは次のブートまで無効のままにしてください。これは、アクティブディレクトリドメインに参加するときに特に重要です。FBWFを無効または有効にする手順については、「File Based Write Filter(FBWF)の使用方法」を参照してください。

ドメイン変更を永続的にするには、以下の手順を実行します。

1. FBWFを無効にします。
2. ドメインに参加します。
3. US300cをリブートします。
4. FBWFを有効にします。
5. US300cをリブートします。

[FBWF を有効]アイコンを使用してFBWFを有効にすると、2回目のリブートは自動的に実行されます。
デフォルトでは、US300cの起動時またはユーザーのログオフ時にNetXCleanユーティリティが、特に選択したシステム上のプロファイルを除くすべてのデータを消去します。NetXCleanユーティリティで新しいプロファイルを消去しないようにする方法については、「NetXCleanユーティリティについて」を参照してください。

ローミングプロファイルの使用方法

Cドライブにローミングプロファイルを書き込むことにより、ドメインに参加できます。プロファイルのサイズを制限する必要があります。また、プロファイルは、US300cの再起動時に失われます。

ローミングプロファイルを正常にダウンロードし正しく機能させるためには、ローミングプロファイル用に十分なフラッシュメモリ容量が必要です。ローミングプロファイル用の容量を確保するためにソフトウェアコンポーネントの削除が必要となる場合があります。

WinPing診断ユーティリティの使用方法

WinPingは、Windows PING(Packet Internet Groper)診断ユーティリティを起動し、pingからの結果を表示するために使用します。[WinPing]ウィンドウを開くには、[スタート]→[ファイル名を指定して実行]をクリックして、[名前]テキストボックスに「WinPing」と入力し、[OK]をクリックします。

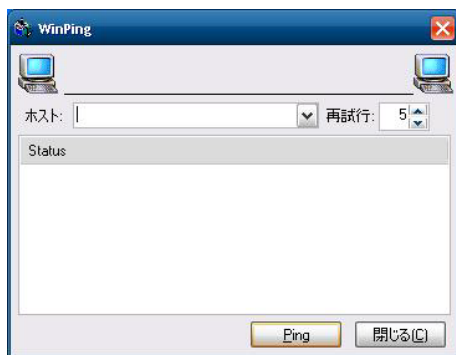



図7-14　WinPing

WinPingは、ネットワークホストにエコー要求を送信する診断ツールです。[ホスト]パラメータには、有効なホスト名またはIPアドレスが入ります。ホストが動作可能な状態でネットワーク上に存在する場合は、エコー要求に応答します。デフォルトでは5回エコー要求を送信し、応答が検出されない場合は送信を停止します。WinPingは1秒に1回エコー要求を送信し、往復時間およびパケット損失の統計を計算し、完了時に短い要約を表示します。

WinPingは、以下の目的で使用します。

- ネットワークおよび各ホストの状態を判断する
- ハードウェアおよびソフトウェアの問題を追跡し、切り分ける
- ネットワークのテスト、評価、および管理を行う
- 名前のみ分かっているホストのIPアドレスを特定する

ユーザーマネージャによるユーザーとグループの管理

ユーザーマネージャを使用して、管理者は新しいユーザーアカウントを作成し、ユーザープロファイルを設定できます。また、新しいグループを作成し、グループにメンバーを割り当てることができます。デフォルトでは、新しいユーザーはUsersグループのメンバーとなり、何も設定されていない状態です。管理者は、新しいユーザーの属性およびプロファイル設定を選択する必要があります。

重要

デフォルトでは、すべてのアプリケーション設定がCドライブのキャッシュに保存されるように設定されています。FBWFキャッシュのオーバーフローを避けるために、RAMディスク(Zドライブ)へのキャッシュを(ユーザーおよび管理者アカウントでデフォルトに設定されているとおり)強くお勧めします。

新しいユーザーアカウントの作成

VNCによってローカルまたはリモートで新しいユーザーアカウントを作成できるのは管理者のみです。ローカルフラッシュメモリやディスク容量上の制約により、追加ユーザー数は最小限に抑えることをお勧めします。

重要

新しいアカウントを作成するカレントシステムセッション中に必ずFBWFキャッシュのファイルを一括書き込みしてください。

以下のガイドラインに従ってください。

1. 管理者としてログオンし、ユーザーマネージャを開きます([スタート]→[コントロールパネル]→[管理ツール]→[User Manager])。
2. [ユーザー]フォルダ→メニューバーの[操作]→[新しいユーザー]をクリックして[新しいユーザー]ダイアログボックスを開きます。
3. ユーザー情報および認証情報を入力し、そのユーザーに必要な属性を選択し、[作成]をクリックします(引き続き必要な数だけユーザーを作成できます)。
4. 必要なユーザーを作成後、[閉じる]をクリックします。作成したユーザーがユーザーペインのリストに表示されます。

ユーザープロファイルの設定

ユーザーのプロファイル設定を選択できるのは、管理者のみです。

フラッシュメモリのサイズが限られているため、新規ユーザーと既存のユーザーが使用できる他のアプリケーションでローカルファイルシステムへの書き込みを防ぐように設定することを強くお勧めします。同じ理由から、出荷時にインストールされているアプリケーションの設定を変更する場合は特にご注意ください。

以下のガイドラインに従ってください(Administratorsグループにユーザーを追加する例)。

重要

アカウントを変更するカレントシステムセッション中に必ずFBWFキャッシュのファイルを一括書き込みしてください。

1. 管理者としてログオンし、ユーザーマネージャを開きます([スタート]→[コントロールパネル]→[管理ツール]→[User Manager])。
2. [ユーザー]フォルダをクリックし、任意のユーザーをダブルクリックして[任意のユーザーのプロパティ]ダイアログボックスを開き、[所属するグループ]タブをクリックします。
3. [追加]をクリックし、[グループの選択]ダイアログボックスを表示します。
4. [選択するオブジェクト名を入力してください]テキストボックスに「Administrators」と入力し、[名前の確認]コマンドボタンをクリックします。
5. [選択するオブジェクト名を入力してください] テキストボックスの内容が「(フルコンピュータ名)¥Administrators」に変更されたことを確認したら、[OK]をクリックします。これで、ユーザーはAdministratorsとUsersの両方のグループのメンバーになります。

新しいグループの作成

VNCによってローカルまたはリモートで新しいグループを作成できるのは管理者のみです。ローカルフラッシュメモリやディスク容量上の制約により、追加グループ数は最小限に抑えることをお勧めします。

重要

新しいアカウントを作成するカレントシステムセッション中に必ずFBWFキャッシュのファイルを一括書き込みしてください。

以下のガイドラインに従ってください。

1. 管理者としてログオンし、ユーザーマネージャを開きます([スタート]→[コントロールパネル]→[管理ツール]→[User Manager])。
2. [グループ]フォルダ→メニューバーの[操作]→[新しいグループ]をクリックして[新しいグループ]ダイアログボックスを開きます。
3. グループの名前および説明を入力し、[作成]をクリックします(引き続き必要な数だけグループを作成できます)。
4. 必要なグループを作成後、[閉じる]をクリックします。作成したグループがグループペインのリストに表示されます。

グループにユーザーを追加する場合

以下のガイドラインに従ってください(Administratorsグループにユーザーを追加する例)。

重要 **アカウントを変更するカレントシステムセッション中に必ずFBWFキャッシュのファイルを一括書き込みしてください。**

1. 管理者としてログオンし、ユーザーマネージャを開きます([スタート]→[コントロールパネル]→[管理ツール]→[User Manager])。

2. [グループ]フォルダをクリックし、[Administrators]をダブルクリックして[Administratorsのプロパティ]ダイアログボックスを開き、[追加]をクリックして[ユーザーの選択]ダイアログボックスを開きます。

3. [選択するオブジェクト名を入力してください]テキストボックスに任意のユーザー名を入力し、[名前の確認]コマンドボタンをクリックします。

4. [選択するオブジェクト名を入力してください]テキストボックスの内容が「(フルコンピュータ名)¥(任意のユーザー名)」に変更されたことを確認したら、[OK]をクリックします。これで、任意のユーザーはAdministratorsとUsersの両方のグループのメンバーになります。

US300cのコンピュータ名の変更

US300cのコンピュータ名を変更できるのは、管理者のみです。

コンピュータ名情報およびターミナルサービスクライアントアクセスライセンス（TSCAL）は、FBWFの有効／無効にかかわらず保持されます。このため、特定のコンピュータを識別する情報は維持され、US300cのイメージをより簡単に管理できます。

以下のガイドラインに従ってください。

1. 管理者としてログオンし、[システムのプロパティ]ダイアログボックスを開きます([スタート]→[コントロールパネル]→[システム])。
2. [コンピュータ名]タブをクリックします。
3. [変更]をクリックします。
4. 新しいコンピュータ名を入力し、[OK]をクリックします。

追加ソフトウェアの利用

US300cに別途ソフトウェアをインストール・アンインストールする方法について説明します。

ソフトウェアのインストール方法

1. US300cを起動します。
2. "Administrator"アカウントでログインしてください。
3. デスクトップに配置されている、[FBWF を無効]アイコンをダブルクリックします。
4. 自動的に再起動されます。(再起動後、FBWFが無効化され、アプリケーションのインストールが可能となります。)
5. 再起動後、再度"Administrator"アカウントでログインしてください。
6. 使用するソフトウェアのインストールを行ってください。
7. インストールが完了しましたら、US300cを再起動してください。
   ※ 自動的に再起動を行わないアプリケーションの場合でも、再起動を行ってください。
8. 再起動後、再度"Administrator"アカウントでログインしてください。
9. インストールしたアプリケーションで何か設定が必要な場合は、設定を行ってください。
   ※ 以降の手順で、FBWFを有効化しますので、設定の変更が再起動時に破棄されます。
   ここで設定した内容については、FBWF有効後も保持されます。
   再度設定を変更する場合は、FBWFを一旦無効化した状態で実施する必要があります。
10. デスクトップに配置されている[FBWF を有効]アイコンをダブルクリックします。
11. 自動的に再起動されます。(再起動後、FBWFが有効化されます。)

ソフトウェアのアンインストール方法

1. US300cを起動します。
2. "Administrator"アカウントでログインしてください。
3. デスクトップに配置されている、[FBWF を無効]アイコンをダブルクリックします。
4. 自動的に再起動されます。(再起動後、FBWFが無効化され、アプリケーションのアンインストールが可能となります。)
5. 再起動後、再度"Administrator"アカウントでログインしてください。
6. ソフトウェアのアンインストールを行ってください。
7. アンインストールが完了しましたら、US300cを再起動してください。
   ※ 自動的に再起動を行わないアプリケーションの場合でも、再起動を行ってください。
8. 再起動後、再度"Administrator"アカウントでログインしてください。

9. デスクトップに配置されている[FBWF を有効]アイコンをダブルクリックします。

10. 自動的に再起動されます。（再起動後、FBWFが有効化されます。）

重要

- **ソフトウェアをインストール・アンインストールする前にFBWFを無効化してください。**
- **ソフトウェアをインストール・アンインストールした後はFBWFを有効化してください。**
- **インストーラによっては、空き容量不足のエラーが表示されインストールが出来ない場合があります。**

  その場合は、下記の【RAM DISKの容量を変更する】を参照しRAM DISKの容量を変更してください。

RAM DISKの容量を変更する

1. US300cを起動します。

2. "Administrator"アカウントでログインしてください。

3. デスクトップに配置されている、[FBWF を無効]アイコンをダブルクリックします。

4. 自動的に再起動されます。（再起動後、FBWFが無効化され、アプリケーションのアンインストールが可能となります。）

5. 再起動後、再度"Administrator"アカウントでログインしてください。

6. コントロールパネルを開き、[Ramdisk]を実行してください。

7. [Ramdisk Configuration]ダイアログが表示されますので、Ramdiskサイズを変更し、[OK]ボタンを押下してください。
   ※ デフォルトは30MBで、最大値は、100MBです。

8. サイズを変更後、US300cを再起動して下さい。

9. 再起動後、再度"Administrator"アカウントでログインしてください。

10. Ramdiskのサイズが変更されていることを確認してください。

11. デスクトップに配置されている[FBWF を有効]アイコンをダブルクリックします。

12. 自動的に再起動されます。（再起動後、FBWFが有効化されます。）

8 システム管理

システム管理について説明しています。

Wyse Device Managerソフトウェアを使用したリモート管理

Wyse Device Manager™ (WDM)サーバーは、ネットワーク管理サービスをUS300cに提供します(リモートシャドー、リブート、シャットダウン、ブート、名前変更、自動デバイスチェックインサポート、Wake-On-LAN、デバイスプロパティの変更などの機能による完全なユーザーデスクトップ管理)。

WDMプロパティの設定については、「WDMプロパティの設定」を参照してください。

WDMがアクセスできるローカルカスタムフィールドについては、「カスタムフィールドによる設定文字列の設定」を参照してください。

アドオンのインストールとアップグレード

アドオンをインストールまたはアップグレードする場合は、WDMを使用することをお勧めします(US300cにはWDM Agentが内蔵されています(「WDMプロパティの設定」を参照してください))。

Wyse Device Managerソフトウェアについては、WyseのWebサイト(http://www.wyse.com/products/software/rapport/)を参照してください。
アドオンはWyseから提供されており、無償のものと有償のものがあります。利用可能なWyseアドオンについては、WyseのWebサイト(http://www.wyse.com/products/software/firmware/)を参照してください。

FTP Addon Installerを使用したアドオンのインストールとアップグレード

US300cの簡単なリモートネットワーク管理サービスを行うにはWDMがお勧めですが、[FTP Addon Installer]ダイアログボックス(管理者のみ使用可能)を使用すると、Microsoft .msi形式のアドオンをインストールおよびアップグレードできます。FTP Addonsユーティリティを使用して指定のFTPサーバーからMSIパッケージをダウンロードすることにより、手動または自動でUS300cにアドオンをインストールまたはアップグレードできます。

一時的なデータ保存用のRAMディスクのサイズの設定については、「RAMディスクサイズの設定」を参照してください。

アドオンの手動インストールとアップグレード

以下のガイドラインに従ってください。

1. 管理者としてログオンし、[FTP Addon Installer]ダイアログボックスを開きます([スタート]→[コントロールパネル]→[FTP Addons])。

システム管理

図8-1　[FTP Addon Installer]ダイアログボックス - 手動設定の例

2. [Manual FTP Information]と[Use DHCP Server's FTP Options]のどちらかを選択して、以下の該当する手順を実行します。

   - [Manual FTP Information]を選択した場合、アドオンをインストールするMSIパッケージのパスとともに、FTPサーバーのIPアドレスを入力します(FTPサーバー上のMSIパッケージと同じパス上にParams.iniファイルが存在している必要があります。Params.iniファイルがないと、インストールは失敗します)。
   - [Use DHCP Server1s FTP Options]を選択した場合、[FTP Path]テキストボックスは無効となり、DHCPサーバーから取得されるFTPサーバー名およびパスが表示されます(「FTPファイルサーバーの使用方法」を参照し、DHCPオプション161(FTPサーバーリスト)および162(FTPファイルへのルートパス)を設定する必要があります)。

3. 認証情報を入力し、FTPサーバーに接続します(デフォルトのユーザー名は「anonymous」で、デフォルトのパスワードは「NEC」です)。

4. 認証情報を入力せずにFTPサーバーへログオンできるように[Save Password]を選択します。

5. (任意設定)[Settings]をクリックして[Network Configurable Settings]ダイアログボックスを開き、接続再試行回数と再試行の間隔を設定します。

6. [Upgrade]をクリックし、FTPサーバーからアドオンをダウンロードします。

[Upgrade]をクリックすると、US300cがリブートされ、Write Filterが無効になります。リブート処理には約5秒 かかります。インストール後、US300cがリブートされ、Write Filterが有効になります。

アドオンの自動インストールとアップグレード

以下のガイドラインに従ってください。

1. 管理者としてログオンし、[FTP Addon Installer]ダイアログボックスを開きます([スタート]→[コントロールパネル]→[FTP Addons])。

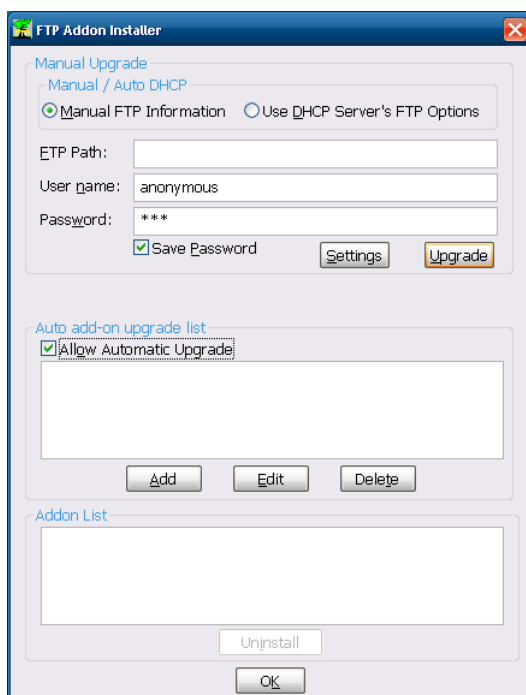



図8-2 [FTP Addon Installer]ダイアログボックス - 自動設定の例

2. [Manual FTP Information]と[Use DHCP Server1s FTP Options]のどちらかを選択して、以下の該当する手順を実行します。

   - [Manual FTP Information]を選択した場合、アドオンをインストールするMSIパッケージのパスとともに、FTPサーバーのIPアドレスを入力します(FTPサーバー上のMSIパッケージには同じパス上にあるParams.iniファイルを付ける必要があります。Params.iniファイルがないと、インストールは失敗します)。
   - [Use DHCP Server1s FTP Options]を選択した場合、[FTP Path]テキストボックスは無効となり、FTPサーバー名およびDHCPサーバーからのパスが表示されます(「FTPファイルサーバーの使用方法」を参照し、DHCPオプション161(FTPサーバーリスト)および162(FTPファイルへのルートパス)を設定する必要があります)。

3. 認証情報を入力します(デフォルトのユーザー名は「anonymous」で、デフォルトのパスワードは「NEC」です)。

4. 認証情報を入力せずにFTPサーバーにログオンできるように[Save Password]を選択します。

5. (任意設定)[Settings]をクリックして[Network Configurable Settings]ダイアログボックスを開き、接続再試行回数と再試行の間隔を設定します。

6. [Allow Automatic Upgrade]チェックボックスにチェックします。[Add]、[Edit]、[Delete]ボタンがアクティブになります。

7. [Add]をクリックし、[Add-on Upgrade FTP Info]ダイアログボックスを使用して(必要な場合は、MSIパッケージの[FTP Path]にFTPサーバーへのパスを入力し、ユーザー名とパスワードを入力)、新しいアドオンを[Auto add-on upgrade list]に追加します。

8. (任意設定)アドオンの情報を変更するには、[Auto add-on upgrade list]でアドオンを選択して[Edit]をクリックします。

9. (任意設定)リストからアドオンを削除するには、[Auto add-on upgrade list]でアドオンを選択して[Delete]をクリックします。

10. 設定を完了後、[OK]をクリックし、US300cをリブートします。FTP Addonsユーティリティは[Auto add-on upgrade list]をチェックし、リスト内のアドオンがインストールされていない場合や、インストール済みのアドオンの最新バージョンが提供されている場合は、US300cがリブートされてWrite Filterが無効になり、アドオンのインストールまたはアップグレードが実行されます。インストール完了後、US300cがリブートされ、Write Filterが有効になります。

FTP Addonsユーティリティは、US300cが再起動される度に[Auto add-on upgrade list]内のすべてのアドオンに対し、最新バージョンの有無を自動的にチェックします。

FTP Addon Installerを使用したアドオンのアンインストール

FTP Addonsユーティリティでインストールした US300cのアドオンは、[FTP Addon Installer]ダイアログボックスを使用してアンインストールできます。

以下のガイドラインに従ってください。

1. 管理者としてログオンし、[FTP Addon Installer]ダイアログボックスを開きます([スタート]→[コントロールパネル]→[FTP Addons])。

2. アンインストールするアドオンを[Addon List]から選択します。

3. [Uninstall]をクリックします。US300cがリブートされ、Write Filterが無効になり、アドオンがアンインストールされます。その後、US300cがリブートされ、Write Filterが有効になります。

[Auto add-on upgrade list]内のアドオンをアンインストールすると、そのアドオンはリストから自動的に削除されます。

Write Filterを無効にした後でWindowsの「プログラムの削除と追加」ユーティリティを使用してアドオンを削除する場合は、US300cをいったんリブートして[FTP Addon Installer]ダイアログボックスの[Addon List]をアップデートし、Write Filterを有効にする必要があります。

US300cでのWindows Server Update Services(WSUS)の使用方法

WSUSを使用して、Windows Embedded Standardを実行するUS300c上にソフトウェアアップデートを自動的に展開する方法を説明します。WSUSを使用してソフトウェアアップデートを展開する前に、サーバーをWSUS用に正しく設定する必要があります。

WSUSを使用するためのUS300cの設定

US300cのWindows Embedded Standardのデフォルトのインストールでは、管理者以外のユーザーはアップデート通知を受け取ることができません。US300c上でアップデート通知の状況を確認するには、以下の手順を実行します。

1. US300cで[スタート]→[ファイル名を指定して実行]をクリックします。[名前] テキストボックスに「gpedit.msc」を入力します。

2. [コンピュータの構成]→[管理用テンプレート]→[Windows Components]→[Windows Update]にナビゲートします。「Allow non-administrators to receive update notifications」オプションまたはGPOが表示されない場合は、US300c上でwuau.admファイルを変更する必要があります。

wuau.admファイルを変更して管理者以外のユーザーがアップデート通知を受け取れるようにするには、以下の手順を実行します。

1. US300cでWrite Filterを無効にします。

2. Windows Server 2003またはWindows Embedded StandardオペレーティングシステムからC:¥windows¥infフォルダにwuau.admファイルをコピーします。

3. US300cでWrite Filterを有効にします。

US300cは、アップデートを配布するサーバー上で設定されているグループまたはGPOの一部である必要があります。

WSUSを使用したUS300c上での自動ソフトウェアアップデート

このセクションでは、WSUSを使用してUS300c上でソフトウェアアップデートを自動的に展開する3つの方法を説明します。

- 「スタンドアロンモードのUS300cでのWSUSの使用」
- 「SMSで自動ソフトウェアアップデートを行うためのWSUSの設定」
- 「WDMと組み合わせたWSUSの使用方法」

スタンドアロンモードのUS300cでのWSUSの使用

US300c上でWSUSを設定し、新しいソフトウェアアップデートを自動的にチェックしてインストールできます。デフォルトでは、US300cは22時間ごとにアップデートをチェックしますが、チェックの間隔を短く設定することもできます(一番短い頻度は1時間です)。アップデートが提供されている場合、US300cは使用可能な帯域幅だけを使用してアップデートをダウンロードします。ユーザーの活動に対する影響はないので、ユーザー通知は行われません(必要な場合は、ユーザー通知を設定することもできます)。

ソフトウェアがUS300cにダウンロードされると、gpedit.mscで設定したポリシーに従ってインストールが実行されます。ポリシーを設定する際には、インストールがユーザーに与える影響を考慮することが重要です。US300cのアップデート後は、常にUS300cのリブートが必要になります。

前提条件

WSUSを使用してソフトウェアアップデートを展開する前には、以下の手順を実行しておく必要があります。

- サーバーにWSUS Server v. 2.0またはWSUS Server v.3.0をインストールします。
- US300cとサーバー間の通信を設定します。

GUIを使用してWSUSを設定するには、以下の手順を実行します。

1. [スタート]→[マイコンピュータ]アイコンを右クリックし、コンテキストメニューから[プロパティ]を選択します。
2. [services.msc]タブをクリックし、Automatic Update Componentと関連するサービスを表示します。
3. WSUSイントラネットサーバーと通信を行うために[Group Policy]を設定します。
4. Windows Embedded StandardクライアントがWSUSサーバーにアクセスすると、保留中のソフトウェアアップデートの通知がタスクバーに表示されます。
5. ソフトウェアアップデートをインストールするには、「VBスクリプトについて」を参照し、スクリプトを実行してインストールの前にWrite Filterを無効にし、インストール完了後に再度有効にします。

必要なアップデートをインストールする前には、Write Filterを無効にする必要があります。Write Filterが有効な場合、US300cは次回リブートされるまでアップデートファイルを保持できますが、リブート時には削除されます。

コマンドラインインタフェースを使用してWSUSを設定するには、以下の手順を実行します。

1. [スタート]メニューから[ファイル名を指定して実行]を選択し、「名前」テキストボックスに[cmd]と入力してコマンドプロンプトを表示します。
2. コマンドプロンプトで「wuauclt.exe」と入力します。
3. 実行可能ファイルを実行し、[Group Policy]を設定してUS300cがWSUSイントラネットサーバーと通信できるようにします。

4. ソフトウェアアップデートをインストールするには、「VBスクリプトについて」を参照し、スクリプトを実行してインストールの前にWrite Filterを無効にし、インストール完了後に再度有効にします。

スタンドアロンモード時のWSUSのトラブルシューティング

WSUSでは、ソフトウェアアップデートに関する問題を解決するためのログを提供します。このログはUS300cのC:¥windows¥windowsupdate.logファイルに出力されます。 このログには、US300cとサーバー間のすべての通信が表示されます。PERFMONを使用すると、アップデートログのWSUSクライアントWebサービスコンポーネントおよびWSUSサーバーWebサービスコンポーネントのメモリ割り当てを監視できます。

ネットワークモニタリングまたはパケットスニッフィングツールを使用して、US300cとサーバー間のトラフィックを監視することもできます。

表2に、WSUSのログの形式の例を示します。

表2 WSUSログの形式

日付	時間	PID	TIDコンポーネント	テキスト
2005-06-01	18:30:03	992	810Misc	= Logging initialized
2005-06-01	18:30:03	992	810Misc	= Process
2005-06-01	18:30:03	992	810Misc	= Module

表3に、WSUSログに書き込むことができるコンポーネントを示します。

表3 WSUSのコンポーネント

コンポーネント	説明
AGENT	Windows Updateエージェント
AU	自動アップデートはこのタスクを実行中です。
AUCLNT	AUによるログオンユーザーとの対話
CDM	デバイスマネージャ
CMPRESS	圧縮エージェント
COMAPI	Windows Update API
DRIVER	デバイスドライバ情報
DTASTOR	データベーストランザクションを処理します。
DWNLDMGR	ダウンロードジョブを作成および監視します。
EEHNDLER	アップデートの適用可能性を評価するために使用する式ハンドラ
HANDLER	アップデートインストーラを管理します。
MISC	全般的なサービス情報
OFFLSNC	ネットワーク未接続時、利用可能なアップデートを検出します。
PARSER	式の情報を構文分析します。
PT	アップデート情報をローカルデータストアに同期させます。
REPORT	レポート情報を収集します。
SERVICE	自動アップデートサービスの起動とシャットダウン
SETUP	Windows Updateクライアントの新しいバージョン提供されている場合、インストールします。
SHUTDWN	シャットダウン時にインストールを実行します。
WUREDIR	Windows Updateリダイレクタファイル
WUWEB	Windows Update ActiveXコントロール

Windows Updateのログファイルの例

以下に、選択した活動に対するログファイルの例を示します。

サービスの起動

2005-06-01 18:30:03 992 810 Service ************* 2005-06-01 18:30:03 992 810 Service ** START ** Service:Service startup 2005-06-01 18:30:03 992 810 Service *********

Windows Updateエージェントが、利用可能なアップデートを検索しています。

2005-06-02 12:09:36 992 4e8 Agent ************* 2005-06-02 12:09:36 992 4e8 Agent ** START ** Agent:Finding updates [CallerId = WindowsUpdate] 2005-06-02 12:09:36 992 4e8 Agent ********* 2005-06-02 12:09:36 992 4e8 Agent * Added update {AC94DB3B-E1A8-4E92-9FD0-E86F355E6A44}.100 to search result 2005-06-02 12:09:37 992 4e8 Agent * Found 6 updates and 10 categories in search

ユーザーが一件のアップデートを提示され、そのインストールを選択しています。

2005-06-02 12:10:41 1660 d0c COMAPI ------------- 2005-06-02 12:10:41 1660 d0c COMAPI -- START -- COMAPI:Install [ClientId = WindowsUpdate] 2005-06-02 12:10:41 1660 d0c COMAPI --------- 2005-06-02 12:10:41 1660 d0c COMAPI - Allow source prompts:Yes; Forced:No; Force quiet:No 2005-06-02 12:10:41 1660 d0c COMAPI - Updates in request:1 2005-06-02 12:10:41 1660 d0c COMAPI - ServiceID = {9482F4B4-E343-43B6-B170-9A65BC822C77} 2005-06-02 12:10:41 1660 d0c COMAPI - Updates to install = 1 2005-06-02 12:10:41 1660 d0c COMAPI <<-- SUBMITTED -- COMAPI:Install [ClientId = WindowsUpdate]

Windows Updateエージェントが、インストール処理を開始しています。

2005-06-02 12:10:41 992 58c Agent ************* 2005-06-02 12:10:41 992 58c Agent ** START ** Agent:Installing updates [CallerId = WindowsUpdate] 2005-06-02 12:10:41 992 58c Agent ********* 2005-06-02 12:10:41 992 58c Agent * Updates to install =

1 2005-06-02 12:10:41 992 58c Agent * Title = <NULL> 2005-06-02

12:10:41 992 58c Agent * UpdateId =

{19813D2E-0144-43CA-AEBB-71263DFD81FD}.100 2005-06-02 12:10:41 992

58c Agent * Bundles 1 updates:2005-06-02 12:10:41 992 58c Agent *

{08D9F87F-7EA2-4523-9F02-0931E291908E}.100

SMSで自動ソフトウェアアップデートを行うためのWSUSの設定

WSUSを設定し、Workgroup環境またはアクティブディレクトリで、SMSサーバーを使用した自動ソフトウェアアップデートを実行できます。

前提条件

WSUSを使用してソフトウェアアップデートを展開する前には、以下の手順を実行しておく必要があります。

- サーバーとUS300cにSMS 2003またはSMS 2007をインストールします。
- サーバーにWSUS Server v. 2.0またはWSUS Server v.3.0をインストールします。
- 「WSUSを使用するためのUS300cの設定」を参照して、US300cでWSUSを使用できるように設定します。

WSUSをSMSと組み合わせてUS300c上で自動ソフトウェアアップデートを実行するには、以下の手順を実行します。

SMSサーバーからSMSサーバーに接続されているUS300cに必要なスクリプト(プレスクリプト)をプッシュします。スクリプトは、以下の処理を行うように設定する必要があります。

1. Write Filterを無効にする。
2. US300c上で対象となるアップデートのダウンロードおよびインストールを開始する。
3. Write Filterを有効にする。

VBスクリプトについて

SMSによるソフトウェア配布では、Windows Embedded Standardシンクライアント上で、アプリケーションの展開前にWrite Filterを無効にする操作とアプリケーションの展開後にWrite Filterを有効にする操作の2つのWrite Filter操作が必要です。実行するVBスクリプトは各操作に1つずつあります。

このVBスクリプトは、プロンプトメッセージを表示せずにUS300c上で実行されます。

Disable_ewf_fbwf.vbsスクリプトはEWFおよびFBWFを無効にし、60秒以内にUS300cを再起動します。再起動後、Write Filterは無効になります。

このスクリプトの実行後、アプリケーションまたはパッチをUS300c上で展開できます。ソフトウェア展開後は、Enable_ewf_fbwf.vbsスクリプトを実行してEWFおよびFBWFを有効にし、60秒以内にUS300cを再起動します。再起動後、Write Filterが有効になります。

チェック

サーバーにWSUS 3.0をインストールしている場合は、US300c上でソフトウェアアップデートの進捗状況を監視し、アップデート完了後にスクリプトをプッシュしてWrite Filterを再度有効にできます。

SMSと組み合わせて使用する際のWSUSのトラブルシューティング

「スタンドアロンモード時のWSUSのトラブルシューティング」で説明しているツールは、SMSと組み合わせてWSUSを使用する場合も使用できます。

また、SMSサーバーのログを使用してパッケージの状態を把握する、WSUSクライアントのログを使用してアップデート時の問題を解決することもできます。

WDMと組み合わせたWSUSの使用方法

WDMを使用してWrite Filterを無効にするスクリプトを展開した後、WSUSサーバーにアクセスしてソフトウェアアップデートをチェックするようにUS300cを設定することができます。

前提条件

WSUSを使用してソフトウェアアップデートを展開する前には、以下の手順を実行しておく必要があります。

- サーバーにWDMをインストールし、設定します。
- サーバーにWSUS Server v. 2.0またはWSUS Server v.3.0をインストールします。
- US300cとサーバー間の通信を設定します。

自動ソフトウェアアップデートを設定するには、以下の手順を実行します。

1. WDMサーバーを使用し、US300c上でWrite Filterを無効にするスクリプトをプッシュします。
2. 「WSUSを使用するためのUS300cの設定」を参照して、WSUSサーバーにアクセスしてソフトウェアアップデートをチェックするようにUS300cを設定します。
3. サーバーでソフトウェアアップデートの状態を監視します。
   - WSUSバージョン2.0では、[WSUS Console]→[Reports]タブで、アップデートの状態を表示できます(図 [WSUS　2.0　Report]タブ を参照)。

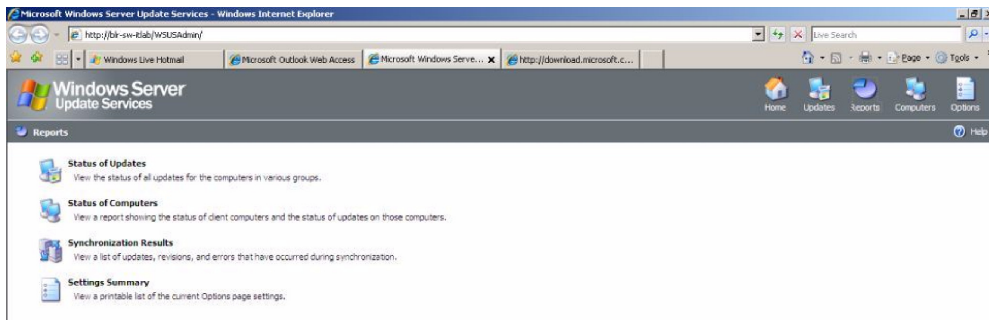



図8-3　[WSUS 2.0 Reports]タブ

- WSUSバージョン3.0では、アップデートのダウンロードを監視するための様々なオプションを備えた、よりグラフィカルなビューを管理コンソールが提供します(図 WSUS 3.0管理コンソール を参照)。

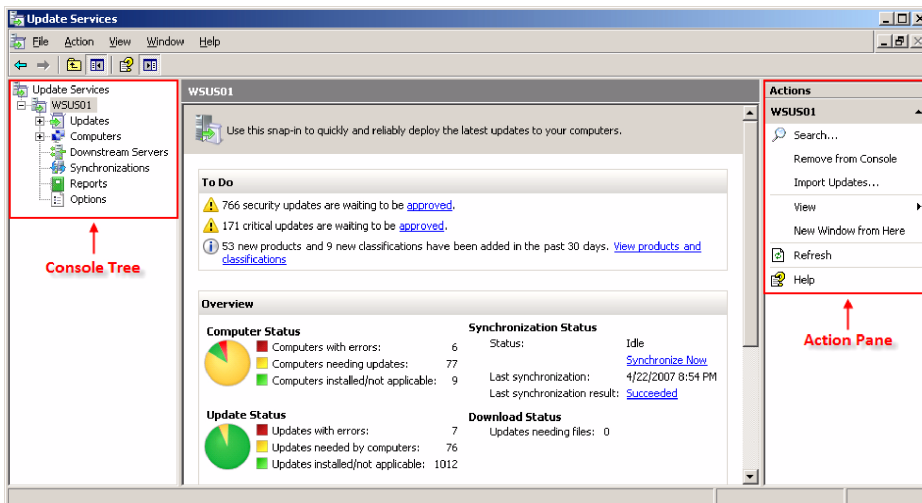



図8-4　WSUS 3.0管理コンソール

4. ソフトウェアアップデートが完了したら、WDMを使用して、Write Filterを有効にするスクリプトをUS300c上で実行するスケジュールを設定します。

ＷＤＭと組み合わせて使用する際のＷＳＵＳのトラブルシューティング

「スタンドアロンモードでのWSUSのトラブルシューティング」で説明している手順で、US300cとサーバーの両方の関連ログを分析することによって、US300cおよびWDMサーバー上のソフトウェアアップデート時の問題を解決することができます。

- **WindowsUpdate.logファイル**

  統計情報を提供します。

- **PERFMONカウンター**

  管理者が使用状況を確認するために使用します。

- **NetmonまたはEtherealトレース**

  データフローを表示します。

- **イベントログ**

  何らかの障害をはじめとするイベントを表示します。

WinVNCを使用したUS300cのリモートシャドー

管理者のみ

WinVNC ServerはUS300cにインストールされています。VNC Serverを使用して、VNC ViewerがインストールされているリモートマシンからUS300cを操作および監視(リモートシャドー)できます。これにより、リモート管理者は、US300cが設置されている場所を実際に訪問しなくても、離れた場所からUS300cを設定またはリセットできます。VNCの主な目的はサポートとトラブルシューティングです。VNC Serverは、US300cの起動時に、サービスとして自動的に起動されます。このサービスは、[サービス]ウィンドウ([スタート]→[コントロールパネル]→[管理ツール]→[サービス])から起動または停止することもできます。

サービスの状態を永続的に保存する場合は、必ずカレントシステムセッション中にFBWFファイルの一括書き込みを行ってください。

VNCサーバーのプロパティの設定

[TightVNC Server: Current User Properties]ダイアログボックスを開くには、[スタート]→[すべてのプログラム]→[WinVNC Current User Properties]をクリックするか、または管理者タスクバーのシステムトレイ内の[TightVNC Server]アイコンをダブルクリックします。VNCの設定については、VNCのマニュアルを参照してください(http://www.realvnc.com)。

このダイアログボックスのデフォルトパスワードは、「NEC」です。
セキュリティ上、US300cを受け取ったらただちにパスワードを変更することを強くお勧めします(管理者として使用する場合のみ)。

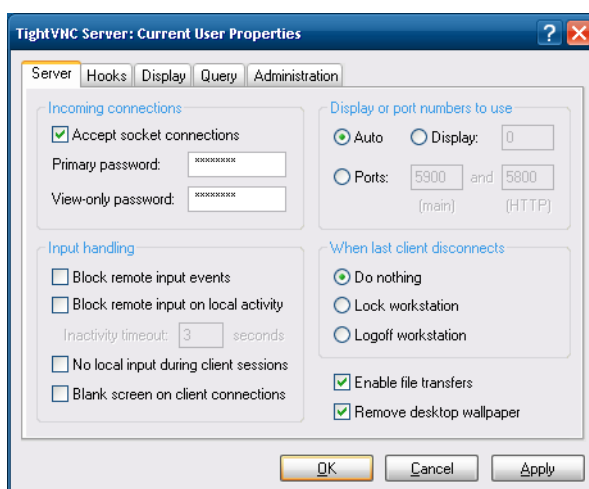



図8-5 [TightVNC Server: Current User Properties]

VNC ViewerがインストールされているリモートマシンでUS300cにアクセスするには、以下の条件が満たされている必要があります。

- リモート管理者またはユーザーが、操作および監視するUS300cのIPアドレス(または有効なDNS名)を把握している必要があります。このIPアドレスは、[ネットワーク接続]ダイアログボックス([スタート]→[コントロールパネル]→[ネットワーク接続]をクリック、[ローカルエリア接続]アイコンをクリックし、左ペインの[詳細]エリアでスクロールダウン)の[詳細]エリア([ローカルエリア接続])で確認できます。

管理者US300cのIPアドレスを見るには、管理者タスクバーのシステムトレイの[TightVNC Server]アイコンの上にマウスポインタを置きます。

- 管理者が使用するパスワードを[TightVNC Server: Current User Properties]ダイアログボックスに入力する必要があります。

VNC Viewerのオプションの設定

VNC ViewerソフトウェアはWDMソフトウェアのコンポーネントに含まれており、リモート(リモートシャドー)マシンにインストールする必要があります。リモートマシンのリモート管理者およびユーザーは、操作および監視するUS300cのIPアドレスや名前、パスワードを把握している必要があります。

UNIX、Linux、Solaris、またはHP-UXマシンを使用してUS300cにリモートアクセスする場合は、対応するVNC Viewerソフトウェアを入手してリモートマシンにインストールする必要があります。VNCソフトウェアについては、VNCのWebサイト(http://www.realvnc.com)を参照してください。

リモート(リモートシャドー)マシンの管理者およびユーザーは、以下の手順でUS300cにログオンできます。

1. [VNC Viewer]アイコンをダブルクリックし、[Connection Details]ダイアログボックスを開きます。

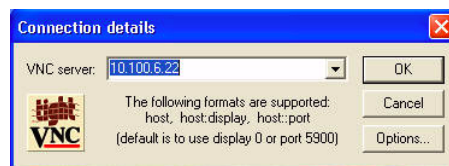



図8-6　VNCの[Connection Details]

2. (任意設定)[Connection Options]ダイアログボックスで高度なVNC接続オプションを設定することもできます。たとえば、ネットワークの速度が遅い場合は、[Options]をクリックして[Connection Options]ダイアログボックスを開き、[Display]エリアの[Restrict Pixels to 8-bit]チェックボックスを選択します(転送速度を改善するために、色深度が小さくなります)。その後、[OK]をクリックして、[Connection Details]ダイアログボックスに戻ります。

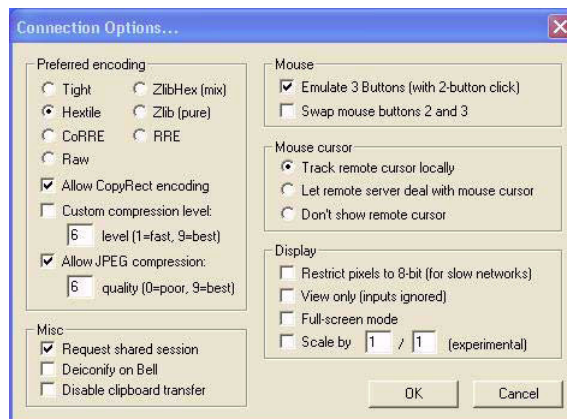



図8-7　[VNC Connection Options]

[VNC Connection Options]ダイアログボックスは、VNCソフトウェアのリリースによって異なります。

以下の一般的なガイドラインに従って設定を行ってください。

- **Preferred encoding**

  通常、VNC Viewerは、CopyRect、Hextile、CoRRE、RREをこの順序で要求します。このオプションで使用するエンコード方式を指定することにより、要求順序を変更できます。

- **Allow CopyRect encoding**

  VNC Viewerは、CopyRectエンコードに対応していることをVNC Serverに伝えます。

- **Request shared session**

  VNC Serverに接続すると、通常、他の既存の接続はすべて終了されます。このオプションは他の接続を維持するので、他のユーザーが使用しているデスクトップを共有できます。

- **Deiconify on Bell**

  電子メールの着信やコンパイル終了などの通知が届くようになるので、頻繁にビープ音が鳴ります。このオプションを選択すると、ベル文字(エスケープシーケンス)を受け取った際に、最小化したVNC Viewerが元のサイズに復元されます。

- **Disable clipboard transfer**

  通常、VNC ViewerまたはVNCサーバーで切り取りまたはコピーが実行されクリップボードが変更されると、この変更はもう一方に転送されます。このオプションを選択すると、クリップボードの転送が無効になります。

- **Emulate 3 Buttons(ボタンが2つのマウスの場合)**

  選択すると、ボタンが2つのマウスを使用しているユーザーが、両方のボタンを同時にクリックすることによって、中央ボタンをエミュレートできます。

- **Swap mouse buttons 2 and 3**

  一般的に、左利きのユーザーが選択するオプションです。

- **Restrict pixels to 8-bit(速度が遅いネットワーク用)**

  選択すると、転送速度を改善するために色深度が小さくなります。

- **View only(入力を無視)**

  リモートシンクライアントのデスクトップを監視するが、キーボードやマウスを使用して操作しない場合は、このオプションを選択します。

- **Full-screen mode**

  フルスクリーンモードで接続を開始します。

3. [Connection Details]ダイアログボックスの[VNC Server]ボックスに、以下のように操作および監視するUS300cのIPアドレスまたは有効なDNS名を入力し、その後にコロンと0を続けます。

snoopy:0

または

132.237.16.238:0

4. [OK]をクリックし、[VNC Authentication]ダイアログボックスを開きます。

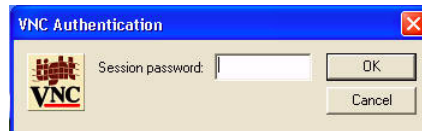



図8-8 [VNC Authentication]

5. 操作および監視するUS300cの[Session password](US300cの[TightVNC Server: Current User Properties]ダイアログボックスで使用するパスワード)を入力し、[OK]をクリックします。

操作および監視するUS300cが、VNC Viewerがインストールされているリモートマシンの別ウィンドウに表示されます。VNC Viewerがインストールされているリモートマシンでマウスやキーボードを使用し、ローカルで操作するのとまったく同じように、操作および監視対象のUS300cを操作してください。

9 運用・保守

US300cの運用および保守について説明しています。

クリーニング

本製品を良い状態に保つために定期的にクリーニングしてください。

⚠警告

本製品を安全にお使いいただくために次の注意事項を必ずお守りください。人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **自分で分解・修理・改造はしない**

本体のクリーニング

本製品の外観の汚れは、柔らかい布でふき取ってください。汚れが落ちにくいときは、次のような方法できれいになります。

重要

- **シンナー、ベンジンなどの揮発性の溶剤は使わないでください。材質のいたみや変色の原因になります。**
- **本製品、コンセント、ケーブル、本製品背面のコネクタ、本製品周辺は絶対に水などでぬらさないでください。**

1. 本製品の電源がOFFになっていることを確認する。
2. 本製品の電源コードをコンセントから抜く。
3. 電源コードの電源プラグ部分についているほこりを乾いた布でふき取る。
4. 中性洗剤をぬるま湯または水で薄めて柔らかい布を浸し、よく絞る。
5. 本製品の汚れた部分を手順4で用意した布で少し強めにこすって汚れを取る。
6. 真水でぬらしてよく絞った布でもう一度ふく。
7. 乾いた布でふく。

トラブルシューティング

複数のシンクライアントを組み合わせて使用する場合のトラブル

PowerPointやWebページの画像や動画が表示されない

→ 仮想PCへの接続をログオフせずに切断状態にして、別のシンクライアントから再接続する場合は、最初の接続と、次の接続の色深度を同じ設定としてください。例えば、最初にUS300cで接続する場合の、接続の色深度が16ビットの場合は、次に接続する別のシンクライアント(例えばUS100、またはWindowsXPのRDPクライアント)の接続の色深度も16ビットとしてください。接続の色深度が一致していない場合、後の接続でPowerPointやWebページ等の画像が表示されない場合があります。色深度が違うシンクライアントから接続する可能性がある場合は、各クライアントでの作業を終える場合は、切断ではなく、仮想PCからログオフする運用としてください。
特にUS100との共存環境では、US100のRDP接続の色設定に15ビットは使用しないでください。15ビットを使用した場合、動画が表示されない場合があります。

RDP/ICA/インターネット時刻等の接続でのトラブル

RDP/ICA/インターネット時刻等の接続に失敗した

→ NetBIOS名で名前解決できなかった場合、完全修飾ドメイン名を指定するようにしてください。

× 接続先：vpc-01
○ 接続先：vpc-01.vpcc.nec.com

プリンタのトラブル

US300cにプリンタを作成してRDP接続しても仮想PCにプリンタが作成されない

→ プリンタドライバの日本語版モデル名と英語版モデル名が異なっている場合、US300cからのRDP接続ではプリンタが作成されません。US300cにプリンタを接続する場合、日本語版と英語版のプリンタドライバでモデル名が同じプリンタをご利用ください。

移動と保管

本製品を移動・保管するときは保守サービス会社に連絡してください。

⚠警告

装置を安全にお使いいただくために次の注意事項を必ずお守りください。人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- 自分で分解・修理・改造はしない

- リチウム電池を取り外さない
- プラグを差し込んだまま取り扱わない

⚠注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、 iiiページ以降の説明をご覧ください。

- 落下注意

重要

- フロアのレイアウト変更など大掛かりな作業の場合はお買い上げの販売店または保守サービス会社に連絡してください。
- 再度、運用する際、内蔵機器や本体を正しく動作させるためにも室温を保てる場所に保管することをお勧めします。
  装置を保管する場合は、保管環境条件(温度:-10～55℃、湿度:20～80%)を守って保管してください(ただし、結露しないこと)。

1. 本体の電源をOFF(POWERランプ消灯)にする。
2. 本体に接続している電源コードをコンセントから抜く。
3. 本体に接続しているケーブルをすべて取り外す。
4. 本体に傷がついたり、衝撃や振動を受けたりしないようしっかりと梱包する。

重要

輸送後や保管後、装置を再び運用する場合は、運用の前にシステム時計の確認・調整をしてください。システム時計を調整しても時間の経過と共に著しい遅れや進みが生じる場合は、お買い求めの販売店、または保守サービス会社に保守を依頼してください。本装置、および、内蔵型のオプション機器は、寒い場所から暖かい場所に急に持ち込むと結露が発生し、そのまま使用すると誤動作や故障の原因となります。装置の移動後や保管後、再び運用する場合は、使用環境に十分なじませてからお使いください。

ユーザーサポート

アフターサービスをお受けになる前に、保証およびサービスの内容について確認してください。

保証について

本装置には『保証書』が添付されています。『保証書』は販売店で所定事項を記入してお渡ししますので、記載内容を確認のうえ、大切に保管してください。保証期間中に故障が発生した場合は、『保証書』の記載内容にもとづき無償修理いたします。詳しくは『保証書』およびこの後の「保守サービスについて」をご覧ください。
保証期間後の修理についてはお買い求めの販売店、最寄りのNECまたは保守サービス会社に連絡してください。

重要

- **弊社製以外(サードパーティ)の製品、または弊社が認定していない装置やインタフェースケーブルを使用したために起きた装置の故障については、その責任を負いかねますのでご了承ください。**
- **本体の底面に、製品の形式、SERIAL No.(号機番号)、定格、製造業者名、製造国が明記された銘板が貼ってあります。販売店にお問い合わせする際にこの内容をお伝えください。また銘板の号機番号と保証書の保証番号が一致していませんと、保証期間内に故障した場合でも、保証を受けられないことがありますのでご確認ください。万一違う場合は、販売店にご連絡ください。**

修理に出される前に

「故障かな？」と思ったら、以下の手順を行ってください。

1. 電源コードおよび他の装置と接続しているケーブルが正しく接続されていることを確認します。
2. 「トラブルシューティング（191ページ）」を参照してください。該当する症状があれば記載されている処理を行ってください。
3. 本装置を操作するために必要となるソフトウェアが正しくインストールされていることを確認します。
4. 市販のウィルス検出プログラムなどでサーバーをチェックしてみてください。

以上の処理を行ってもなお異常があるときは、無理な操作をせず、お買い求めの販売店、最寄りのNECまたは保守サービス会社にご連絡ください。その際にサーバーのランプの表示やディスプレイ装置のアラーム表示もご確認ください。故障時のランプやディスプレイによるアラーム表示は修理の際の有用な情報となることがあります。保守サービス会社の連絡先については、付録C「保守サービス会社網一覧」をご覧ください。
なお、保証期間中の修理は必ず保証書を添えてお申し込みください。

重要

この装置は日本国内仕様のため、NECの海外拠点で修理することはできません。ご了承ください。

修理に出される時は

修理に出される時は次のものを用意してください。

□ 保証書
□ ディスプレイ装置に表示されたメッセージのメモ
□ 障害情報（障害情報は保守サービス会 社から指示があったときのみ用意してください。）
□ 本体・周辺機器の記録

補修用部品について

本装置の補修用部品の最低保有期間は、製造打ち切り後5年です。

保守サービスについて

保守サービスはNECの保守サービス会社、およびNECが認定した保守サービス会社によってのみ実施されますので、純正部品の使用はもちろんのこと、技術力においてもご安心の上、ご都合に合わせてご利用いただけます。
なお、お客様が保守サービスをお受けになる際のご相談は、弊社営業担当または代理店で承っておりますのでご利用ください。保守サービスは、お客様に合わせて2種類用意しております。

保守サービスメニュー

契約保守サービス	お客様の障害コールにより優先的に技術者を派遣し、修理にあたります。この保守方式は、装置に応じた一定料金で保守サービスを実施させていただくもので、お客様との間に維持保守契約を結ばせていただきます。さまざまな保守サービスを用意しています。詳しくはこの後の説明をご覧ください。
未契約修理	お客様の障害コールにより、技術者を派遣し、修理にあたります。保守または修理料金はその都度精算する方式で、作業の内容によって異なります。

NECでは、お客様に合わせてさまざまな契約保守サービスを用意しております。サービスの詳細については、「NEC コーポレートサイト(http://www.nec.co.jp/)」の「サポート情報」をご覧ください。

- **サービスを受けるためには事前の契約が必要です。**
- **サービス料金は契約する日数/時間帯により異なります。**

情報サービスについて

本製品に関するご質問・ご相談は「ファーストコンタクトセンター」でお受けしています。
※　電話番号のかけまちがいが増えております。番号をよくお確かめの上、おかけください。

ファーストコンタクトセンター

TEL. 03-3455-5800(代表)

受付時間／9:00～12:00、13:00～17:00　月曜日～金曜日(祝祭日を除く)

お客様の装置本体を監視し、障害が発生した際に保守拠点からお客様に連絡する「エクスプレス通報サービス」の申し込みに関するご質問・ご相談は「エクスプレス受付センター」でお受けしています。
※　電話番号のかけまちがいが増えております。番号をよくお確かめの上、おかけください。

エクスプレス受付センター

TEL. 0120-22-3042

受付時間／9:00～17:00　月曜日～金曜日(祝祭日を除く)

インターネットでも情報を提供しています。

http://www.nec.co.jp/

NEC コーポレートサイト：製品情報、Q&Aなど最新Express情報満載！

http://club.express.nec.co.jp/

『Club Express』：『Club Express会員』への登録をご案内しています。Express5800シリーズをご利用になる上で役立つ情報サービスの詳細をご紹介しています。

http://www.fielding.co.jp/

NECフィールディング(株)ホームページ：メンテナンス、ソリューション、用品、施設工事などの情報をご紹介しています。

付録A　無線LAN仕様一覧

IEEE802.11b/g

項　目	規　格
準拠規格	IEEE802.11b、 IEEE802.11g
通信モード	IEEE802.11bモード：11/5.5/2/1 (Mbpsモード) *1 IEEE802.11gモード：54/48/36/24/12/9/6 (Mbpsモード) *1
無線チャンネル	1〜11ch
周波数帯域	2.4GHz帯域（2.4〜2.462GHz）

*1：各規格による理論的な通信速度をもとにした通信モード表記であり、実効速度とは異なります。
接続対象機器、電波環境、周囲の障害物、設置環境、使用状況、ご使用のＯＳ、アプリケーション、ソフトウェアなどによっても通信速度、通信距離に影響する場合があります。

IEEE802.11n Draft2.0

項　目	規　格
準拠規格	IEEE802.11n Draft2.0 *1
通信モード	20/40Mbpsモード*2
無線チャンネル	1〜11ch
周波数帯域	2.4GHz帯域（2.4〜2.462GHz）

*1：「IEEE802.11n Draft2.0準拠」の表記は、他のIEEE802.11nDraft対応製品との接続性を保証するものではありません。
*2：各規格による理論的な通信速度をもとにした通信モード表記であり、実効速度とは異なります。
接続対象機器、電波環境、周囲の障害物、設置環境、使用状況、ご使用のＯＳ、アプリケーション、ソフトウェアなどによっても通信速度、通信距離に影響する場合があります。

付録B　仕　様

項　目	仕　様
CPU	VIA EDEN 1GHz
Chipset	VIA VX855
Memory	2GB Flash/1GB RAM DDR2
I/O Ports	1 x DVI-I port, DVI to VGA (DB-15) adapter included 4 x USB 2.0 ports (2 on front, 2 on back) 2 x PS/2 ports 1 x Mic In 1 x Line Out
Networking	10/100/1000 Base-T Gigabit Ethernet
Display	VESA monitor support with Display Data Control (DDC) Dual monitor supported Single: 1600x1200@60Hz, Color depth: 8, 15, 16, 24 or 32bpp, Two independent full resolution frame buffers Dual: 1600x1200@60Hz, Color Depth: 8, 15, 16, 24 or 32bpp.
Audio	Output: 1/8-inch mini jack, full 16 bit stereo Input: 1/8-inch mini jack, 8 bit microphone
External Dimension (mm)	177（W）×21（D）×34（H）
Weight	0.6kg
Power	Worldwide auto-sensing 100-240 VAC, 50/60 Hz. Energy StarR V.5.0 compliant power supply Average power usage with device connected to 1 keyboard with 1 PS/2 mouse and 1 monitor: Under 7 Watts
Temperature Range	Horizontal: 10-35℃ (50-95 °F) Vertical: 10-40℃ (50-104 °F)
Humidity	20% to 80% condensing 10% to 95% non-condensing
OS	Windows Embedded Standard (WES)

付録C　保守サービス会社網一覧

本製品、および関連製品のアフターサービスは、お買い上げのNEC販売店、最寄りのNEC、またはNECフィールディング株式会社までお問い合わせください。下記にNECフィールディングのサービス拠点所在地一覧を示します。
（受付時間：月曜日から金曜日AM9:00～PM6:00　土曜日、日曜日、祝祭日および当社規定の休日を除く）
次のWEBサイトにも最新の情報が記載されています。

http://www.fielding.co.jp/

このほか、NEC販売店のサービス網がございます。お買い上げの販売店にお問い合わせください。
トラブルなどについてのお問い合わせは下記までご連絡ください（電話番号のおかけ間違いにご注意ください）。その他のお問い合わせについては、下表を参照してください。

0120-536-111（フリーダイヤル）

携帯電話からは

0570-064-211（通話料お客様負担）

2010年 7月 現在

都道府県名	拠点名	電話番号	郵便番号	所在地
北海道	札幌支店	011-221-3705	060-0042	札幌市中央区大通西4-1　新大通ビル9F
	東札幌支店	011-833-8640	003-0001	札幌市白石区東札幌1条1-6-33
	釧路営業所	0154-32-7100	085-0016	釧路市錦町5-3　三ッ輪ビル2F
	旭川支店	0166-24-2098	070-0033	旭川市三条通9丁目左1号　明治安田生命旭川ビル1F
	オホーツク営業所	0157-25-7520	090-0024	北見市北四条東3-1-1　富士火災北見ビル3F
	苫小牧営業所	0144-36-3846	053-0022	苫小牧市王子町3-2-23　朝日生命苫小牧ビル2F
	室蘭営業所	0143-46-3180	050-0083	室蘭市東町2-24-4　石井第5ビル3F
	函館支店	0138-54-5642	040-0001	函館市五稜郭町1-14　五稜郭114ビル3F
	道東支店	0155-25-4892	080-0013	帯広市西三条南10-32　日本生命帯広駅前ビル5F
	小樽営業所	0134-24-5685	047-0036	小樽市長橋3-4-14
青森	青森支店	017-735-8501	030-0802	青森市本町1-2-20　青森柳町ビル3Ｆ
	八戸営業所	0178-44-4354	031-0081	八戸市柏崎1-10-2　八戸第一生命ビル1F
	弘前営業所	0172-34-9083	036-8002	弘前市駅前2-2-2　弘前第一生命ビル1F
岩手	盛岡支店	019-635-3011	020-0866	盛岡市本宮3-13-20
	一関営業所	0191-25-6531	021-0041	一関市赤荻字月町218-2
宮城	仙台支店	022-292-1900	984-0051	仙台市若林区新寺1-3-45　AI.Premium 7F
秋田	秋田支店	018-863-7938	010-0951	秋田市山王1-3-29
山形	山形支店	023-631-3502	990-2445	山形市南栄町3-6-34
	鶴岡営業所	0235-25-8386	997-0013	鶴岡市道形町23-31　山庄ビル1階
	米沢営業所	0238-24-1418	992-0027	米沢市駅前3-5-22　かなつビル1F
福島	郡山支店	024-938-5209	963-8022	郡山市西ノ内1-22-13
	福島支店	024-536-3703	960-8074	福島市西中央五丁目6番1号
	いわき営業所	0246-28-8371	970-8034	いわき市平上荒川字桜町34-1
	会津若松営業所	0242-28-7624	965-0818	会津若松市東千石2-1-45
茨城	鹿島営業所	0299-82-4860	314-0014	鹿嶋市光3　住友金属構内
	つくば支店	029-860-2000	305-0821	つくば市春日3-22-8
	水戸支店	029-257-1860	310-0911	水戸市見和3-575-3
栃木	宇都宮支店	028-632-8140	321-0954	宇都宮市元今泉2-7-6
	小山営業所	0285-21-1495	323-0807	小山市城東1-14-12　ウエルストン1ビル1F
群馬	群馬支店	027-255-5461	371-0855	前橋市問屋町2-4-3　アルファビル4F
	太田営業所	0276-45-0666	373-0853	太田市浜町58-24

都道府県名	拠点名	電話番号	郵便番号	所在地
埼玉	さいたま北支店	048-660-1881	331-0812	さいたま市北区宮原町2-85-5
	熊谷営業所	048-527-0597	360-0036	熊谷市桜木町1-1-1　秩父鉄道熊谷ビル4F
	さいたま南支店	048-859-7360	338-0832	さいたま市桜区西堀8-21-35 カタヤマビル3F
	川越支店	04-2955-7695	350-1331	狭山市新狭山2-11-10
	越谷営業所	048-978-9500	343-0042	越谷市千間台東1-7-25　エムケービル1F
千葉	千葉支店	043-221-7660	260-0843	千葉市中央区末広1-12-15
	成田営業所	0476-22-5390	286-0033	成田市花崎町807-1　センチュリー成田ビル
	君津営業所	0439-55-7278	299-1144	君津市東坂田1-3-2　京葉君津ビル3F
	船橋営業所	047-434-1611	273-0012	船橋市浜町2-1-1　ららぽーと三井ビル7F
	柏支店	04-7165-2100	270-1168	我孫子市根戸1740
	印西営業所	0476-46-4250	270-1352	印西市大塚1-9 千葉ニュータウンエネルギーセンター1階
東京	東京中央支店	03-6436-5155	108-0023	港区芝浦4-9-25　芝浦スクエアビル8F
	大森支店	03-3764-0007	140-0013	品川区南大井6-25-3　ビリーヴ大森ビル8F
	渋谷支店	03-5458-3341	150-0032	渋谷区鶯谷町2-3　COMS（コムス）2F
	新宿支店	03-5155-7810	169-0072	新宿区大久保1-3-21　新宿TXビル6F
	日本橋支店	03-3297-0783	104-0032	中央区八丁堀4-5-8　KDX八丁堀ビル2・3F
	江東支店	03-3649-3230	135-0016	江東区東陽2-2-20　住友不動産東陽駅前ビル1F
	秋葉原支店	03-5821-2474	111-0052	台東区柳橋2-19-6　柳橋ファーストビル8F
	神田支店	03-3233-2411	101-0064	千代田区猿楽町2-7-8　住友水道橋ビル8F
	流通サービス部	03-5806-3801	110-0014	台東区北上野2-23-5　住友不動産上野ビル2 号館3 階
	立川支店	042-527-2527	190-0022	立川市錦町2-4-6　住友生命立川ビル3F
	小金井支店	042-385-7666	184-0013	小金井市前原町5-9-7
神奈川	神奈川支店	045-314-7625	220-0004	横浜市西区北幸2-8-4　横浜西口KNビル17F
	横須賀営業所	046-827-3188	238-0004	横須賀市小川町14-1　ニッセイ横須賀センタービル1F
	川崎営業所	044-244-1083	210-0011	川崎市川崎区富士見1-6-3　TOKICO 事務棟ビル3F
	相模支店	042-746-6111	252-0303	相模原市南区相模大野7-1-6　相模大野第一生命ビル4F
	厚木営業所	046-225-0411	243-0018	厚木市中町4-16-21　プロミティあつぎビル5階
	湘南支店	0463-21-4777	254-0035	平塚市宮の前1-2　あいおい損保平塚第一ビル2F
	藤沢営業所	0466-22-0204	251-0055	藤沢市南藤沢17-10　コア湘南田村ビル1Ｆ
	玉川支店	044-814-1551	213-0002	川崎市高津区二子5-1-1　高津パークプラザビル4Ｆ
	小田原営業所	0465-24-7103	250-0011	小田原市栄町一丁目14-52　MANAX ビル6 階
山梨	甲府支店	055-226-7564	400-0858	甲府市相生2-3-16　三井住友海上甲府ビル3Ｆ
	富士吉田営業所	0555-23-9515	403-0007	富士吉田市中曽根3-2-43　ヤマナシ文具センター1Ｆ
長野	松本支店	0263-27-7070	399-0033	松本市笹賀6096-1
	長野支店	026-224-0050	380-0824	長野市南石堂町1293　長栄南石堂ビル5Ｆ
	上田営業所	0268-27-6336	386-0032	上田市諏訪形5-1　豊成ビル5Ｆ
	駒ヶ根営業所	0265-83-1711	399-4117	駒ヶ根市赤穂1298-2　サンポー本社ビル2 階
新潟	新潟支店	025-243-2315	950-0986	新潟市中央区神道寺南2-4-15
	長岡営業所	0258-35-5217	940-0034	長岡市福住2-3-6　小林石油ビル
富山	富山支店	076-442-2605	930-0004	富山市桜橋通り1-18　住友生命富山ビル1Ｆ
	黒部営業所	0765-54-0447	938-0031	黒部市三日市字新光寺1880-1
	高岡営業所	0766-25-4212	933-0912	高岡市丸の内1-40　高岡商工ビル8Ｆ
石川	金沢支店	076-223-3188	920-0919	金沢市南町4-55　住友生命金沢ビル1Ｆ
	小松営業所	0761-24-3782	923-0926	小松市竜助町36　小松東京海上日動ビルディング3Ｆ
福井	福井支店	0776-54-6637	918-8206	福井市北四ツ居町518

都道府県名	拠点名	電話番号	郵便番号	所在地
岐阜	東濃営業所	0572-55-4578	509-5132	土岐市泉町大富261-8
	岐阜支店	058-275-8801	500-8367	岐阜市宇佐南3-4-7
静岡	静岡支店	054-264-6812	422-8004	静岡市駿河区国吉田2-1-20
	富士営業所	0545-64-6735	416-0944	富士市横割1-17-24　FCビル2F
	沼津支店	055-973-6001	411-0906	駿東郡清水町八幡88-1
	浜松支店	053-466-0205	435-0047	浜松市東区原島町111
	掛川営業所	0537-23-2181	436-0222	掛川市下垂木2417　株式会社新開トランスポートシステムズ静岡営業所内2 階
愛知	名古屋支店	052-264-7581	460-0007	名古屋市中区新栄2-28-22　NEC名古屋ビル5F
	名古屋南支店	052-694-1031	457-0862	名古屋市南区内田橋1-8-5　アートライフ・タケセイ1F
	半田営業所	0569-22-2762	475-0903	半田市出口町1-130-1　森田ビル4F
	小牧支店	0568-75-5594	485-0029	小牧市中央1-271　大垣共立銀行小牧支店ビル4F
	岡崎営業所	0564-23-5020	444-0044	岡崎市康生通南3-5　住友生命岡崎第二ビル1F
	豊橋営業所	0532-55-3063	440-0084	豊橋市下地町瀬上83
	三河支店	0565-34-1168	471-0034	豊田市小坂本町1-5-3　朝日生命新豊田ビル3F
三重	三重支店	059-227-1622	514-0042	津市新町3-2-1
	四日市営業所	0593-51-0425	510-0075	四日市市安島1-5-10　KOSCO四日市西浦ビル2F
滋賀	滋賀支店	077-525-3156	520-0043	大津市中央4-5-4　BKビル
京都	京都支店	075-812-5800	604-8804	京都市中京区壬生坊城町24-1　古川勘ビル4F
	京都南営業所	075-642-8021	612-8414	京都市伏見区竹田段ノ川原町28-1 竹田駅前第一ビル3F
	福知山営業所	0773-23-6287	620-0940	福知山市駅南町3-6　竹下駅南ビル2F
大阪	本町支店	06-6264-2810	541-0053	大阪市中央区本町2-1-6　堺筋本町センタービル6F
	大阪支店	06-6264-2828	541-0053	大阪市中央区本町2-1-6　堺筋本町センタービル6F
	北大阪支店	06-6835-0017	560-0083	豊中市新千里西町1-2-2　住友商事千里ビル南館2F
	東大阪支店	072-924-6780	581-0803	八尾市光町1-61　嶋野・住友生命ビル7F
	南大阪支店	072-223-8595	590-0075	堺市堺区南花田口町2-3-20　住友生命堺東ビル南館4F
兵庫	豊岡営業所	0796-24-0331	668-0043	豊岡市桜町15-1　幸栄ビル1F
	神戸支店	078-332-5431	650-0031	神戸市中央区東町126　神戸シルクセンタービル3F
	姫路支店	079-289-2684	670-0948	姫路市北条宮の町113
奈良	奈良支店	0742-36-1161	630-8001	奈良市法華寺町219-1
和歌山	和歌山支店	073-428-3222	640-8154	和歌山市六番丁5　和歌山第一生命ビル
鳥取	鳥取営業所	0857-25-6322	680-0845	鳥取市富安2-159　久本ビル4F
	米子営業所	0859-22-8280	683-0805	米子市西福原2-1-1　YNT第10ビル2階
島根	山陰支店	0852-21-0988	690-0049	松江市袖師町2-38　NKTビル7F
	浜田営業所	0855-22-6092	697-0033	浜田市朝日町70-5　朝日第2ビル1F
岡山	岡山支店	086-246-9606	700-0986	岡山市北区新屋敷町1-1-18　新聞製作センター4 階
	倉敷営業所	086-426-1371	710-0057	倉敷市老松町4-6-11
	津山営業所	0868-31-2821	708-0023	津山市大手町6-8　城南ビル4F
広島	広島支店	082-248-4222	730-0042	広島市中区国泰寺町2-5-11　西橋屋ビル4F
	呉営業所	0823-21-5129	737-0051	呉市中央1-6-9　センタービル呉駅前6F
	東広島営業所	0824-22-6411	739-0015	東広島市西条栄町10-27　栄町ビル2F
	福山営業所	084-931-8907	720-0973	福山市延広町1-25　明治安田生命福山駅前ビル8F

都道府県名	拠点名	電話番号	郵便番号	所在地
山口	山口支店	083-973-1858	754-0011	山口市小郡御幸町4-9　山陽ビル小郡1F
	山口周防営業所	0833-44-1621	744-0011	下松市西豊井1375-3
	岩国営業所	0827-22-9534	740-0012	岩国市元町1-1-17　デミオ元町3F
	下関営業所	0832-57-2939	751-0877	下関市秋根東町8-10　トワムールエクスビル3F
徳島	徳島支店	088-622-1270	770-0852	徳島市徳島町2-19-1　あいおい損保徳島第一ビル4F
香川	高松支店	087-833-1708	760-0008	高松市中野町29-2　高松パークビル7F
	丸亀営業所	0877-23-8563	763-0034	丸亀市大手町3-5-18　ジブラルタ生命丸亀ビル7F
愛媛	松山支店	089-945-4145	790-0878	松山市勝山町1-19-3　青木第一ビル5Ｆ
	八幡浜営業所	0894-23-0173	796-0010	八幡浜市江戸岡一丁目4-6　江戸岡ビル2F
	宇和島営業所	0895-24-1471	798-0032	宇和島市恵美須町2-4-14　井上ビル
	今治営業所	0898-31-5741	794-0063	今治市片山1-2-20
	新居浜営業所	0897-34-4772	792-0003	新居浜市新田町3-2　新居浜ビル5F
	川之江営業所	0896-58-6208	799-0113	四国中央市妻鳥町1010番地8　共和ビル102号室
高知	高知支店	088-873-8851	780-0870	高知市本町4-2-40　ニッセイ高知ビル3F
福岡	福岡支店	092-472-2853	812-0004	福岡市博多区榎田2-3-27　STS第二ビル3F
	北九州支店	093-522-0581	802-0014	北九州市小倉北区砂津1-5-34　小倉興産23号館4F
	飯塚営業所	0948-24-0919	820-0066	飯塚市大字幸袋526-1　福岡ソフトウェアセンター2F
	久留米営業所	0942-44-5298	839-0809	久留米市東合川2-4-29
	大牟田営業所	0944-51-2655	836-0843	大牟田市不知火町2-7-1　中島物産ビル5F
佐賀	佐賀支店	0952-31-9301	849-0937	佐賀市鍋島3-2-19
	佐賀西営業所	0955-21-0990	848-0045	伊万里市松島916　カルフール101
長崎	長崎支店	095-820-0525	850-0032	長崎市興善町6-5　興善町イーストビル4F
	佐世保営業所	0956-34-3811	857-1161	佐世保市大塔町1266-24
	諫早営業所	0957-23-0471	854-0016	諫早市高城町5-10　諫早商工会館5F
	五島営業所	0959-75-0876	853-0033	五島市木場町252番地8　Fビル1F
熊本	熊本支店	096-383-6777	862-0925	熊本市保田窪本町1-40
大分	大分支店	097-503-2555	870-0921	大分市萩原4-9-65
	中津営業所	0979-23-1182	871-0058	中津市豊田町2-423-10　6 BILL 5F
宮崎	宮崎支店	0985-27-4477	880-0806	宮崎市広島1-18-7　大同生命宮崎ビル9F
	延岡営業所	0982-35-7545	882-0847	延岡市旭町3-1-1 旭化成ネットワークス（株）本社棟1F
	都城営業所	0986-27-1702	885-0071	都城市中町1-7　BTV IT産業ビル7F
鹿児島	鹿児島支店	099-285-2266	890-0062	鹿児島市与次郎2-4-35　KSC鴨池ビル1F
	出水営業所	0996-62-8922	899-0202	出水市昭和町13-1　第二丸久ビル2F
沖縄	沖縄支店	098-876-2788	901-2112	浦添市沢岻2-17-1

索　引

W

ア

カ

サ

<本製品の利用目的について>

本製品は、高速処理が可能であるため、高性能コンピュータの平和的利用に関する日本政府の指導対象になっております。
ご使用に際しましては、下記の点につきご注意いただけますよう、よろしくお願いいたします。

1. 本製品は不法侵入、盗難等の危険がない場所に設置してください。
2. パスワード等により適切なアクセス管理をお願いいたします。
3. 大量破壊兵器およびミサイルの開発、ならびに製造等に関わる不正なアクセスが行われるおそれがある場合には、事前に弊社相談窓口までご連絡ください。
4. 不正使用が発覚した場合には、速やかに弊社相談窓口までご連絡ください。

弊社相談窓口　　ファーストコンタクトセンター
電話番号　03-3455-5800

注　意

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。　VCCI-B

回線への接続について

本製品を公衆回線や専用線に接続する場合は、本製品に直接接続せず、技術基準に適合し認定されたボードまたはモデム等の通信端末機器を介して使用してください。

電源の瞬時電圧低下対策について

本製品は、落雷等による電源の瞬時電圧低下に対し不都合が生じることがあります。電源の瞬時電圧低下対策としては、交流無停電電源装置（UPS）等を使用されることをお勧めします。

海外でのご使用について

本製品は、日本国内での使用を前提としているため、海外各国での安全規格等の適用を受けておりません。したがって、本製品を輸出した場合に当該国での輸入通関および使用に対し罰金、事故による補償等の問題が発生することがあっても、弊社は直接・間接を問わず一切の責任を免除させていただきます。